BACHELOR'S THESIS

Degree in Mathematics

Title: Class field theory

Author: Raúl Alonso Rodríguez

Advisor: Francesc Fité Naya

Department: Mathematics

Academic year: 2017-18

UNIVERSITAT POLITÈCNICA DE CATALUNYA
BARCELONATECH
Facultat de Matemàtiques i Estadística

Class field theory

Raúl Alonso Rodríguez

Advisor: Francesc Fité Naya

July 4, 2018

Contents

Acknowledgements

First of all, I would like to express my full indebtedness to Francesc Fité for his absolute dedication to this project. His guidance and advice throughout all these months have been extremely helpful in going through the wonderful but often arduous paths of algebraic number theory. I also want to express my gratitude to the members of the Number Theory research group in Barcelona for all the opportunities to learn with which they have provided me. I would like to make a special mention of Victor Rotger and Óscar Rivero for their helpfulness and always wise advice. I also want to thank all the excellent teachers which I have had during the last four years at UPC, and, in particular, Jordi Quer, for all what I have learned from him on those courses more related to Number Theory. I would like to express my gratitude to the staff at CFIS for always making things easier. And last, but not least, to my family and friends for their continuous support.

Introduction

Class field theory provides a description of the Abelian extensions of local and global fields in terms of the arithmetic of the field itself. This branch of algebraic number theory was mainly developed in the 20th century and is deemed one of the major achievements in the area. At its initial stage, it was developed thanks especially to Takagi and Artin. These first results concerned only global class field theory, stated in terms of generalized ideal class groups, and the proofs strongly depended on analysis. It was not until 1930 that Hasse first introduced local class field theory. The introduction of idèles by Chevalley provided the means to pass from the local to the global results, as well as a more unified version of class field theory: both in the local and global case, we have a one-to-one correspondece between finite Abelian extensions of a field and open subgroups of finite index of a certain topological group, which is the multiplicative group of the field itself in the case of local fields and the idèle class group in the case of global fields. Moreover, the use of this tool allowed to give purely algebraic proofs of the main results in class field theory. The introduction by Tate of what is known as Tate cohomology (a slight modification of classical group cohomology which allows to relate cohomology and homology groups) allowed to give an elegant reformulation of class field theory (which could now be understood in terms of the Tate cohomology groups associated to a certain extension of fields) as well as a new and powerful algebraic tool.

The objective of this thesis is to present and prove the main results of class field theory. There is a strong contrast between the simplicity of the main statements of class field theory (especially in the classical ideal-theoretic formulation) and the hardness of the proofs. In fact, the proofs might seem lengthy and at some points quite technical, but they also introduce fresh and fruitful ideas in the field and are frequently interesting by themselves. This thesis aims to be exhaustive at this point, trying to cover all the proofs of the main results. The chosen approach is based on two principles:

1. It should be possible to obtain the global results from the local results.
2. It should be possible to obtain results which are purely algebraic by purely algebraic methods.

As we have explained, this was not the historical approach, but it has been the most common approach in modern presentations of the topic since Chevalley, and it seems more natural from an algebraic perspective. In fact, it is highly satisfactory that class field theory could be developed according to these two priniciples. This is not always the case; for example, Hasse principle (the existence of global rational solutions to an algebraic equation from the existence of local rational solutions) is not always valid, and there is no known purely algebraic proof of the fundamental theorem of algebra. In our presentation, we strongly rely on Tate cohomology to prove the main theorems, following the theory developed by Tate.

In Chapter 1, the first seven sections briefly present the main results of classical group cohomology and homology. This is the only part in the thesis where proofs are omitted. The other

two sections of this chapter are devoted to introduce continuous cohomology for profinite groups and Tate cohomology. The main result in this chapter is without a doubt Tate's theorem.

In Chapter 2 we present some basic notions regarding valuations and local fields. Valuation theory will allow us to regard the classical prime ideals of a number field and its complex embeddings in a unified way, which will help us bridge the gap from local to global class field theory. This chapter is completely independent from the previous one, and can be skipped by those who are already familiar with the matter.

In Chapter 3 we develop local class field theory following the cohomological approach introduced by Tate. We prove the existence of a local Artin map (what is commonly known as the Reciprocity Law). This is achieved by using Tate's theorem. To verify the hypothesis of this theorem, we are led to introduce the invariant map, which will also be used later.

In Chapter 4 we introduce idèles for number fields, which, together with valuation theory, is the necessary tool to pass from local class field theory to global class field theory.

In Chapter 5 we develop the idelic version of global class field theory. We restrict to the case of number fields. In our approach, we start by directly defining the global Artin map and afterwards we prove that it satisfies the desired requirements, i.e. the global Reciprocity Law. We also prove the global Existence Theorem. This chapter probably contains the hardest and most technical proofs in this thesis.

In Chapter 6 we establish the link between the idelic version of global class field theory developed in the previous chapter and the classical ideal-theoretic version.

Finally, Chapter 7 is devoted to some applications of class field theory. The first of this applications is a simple proof of Kronecker-Weber theorem, which states that any finite Abelian extension of $\mathbb{Q}$ is contained within a certain cyclotomic extension. In fact, this theorem had already been proved using more elementary techniques, but using class field theory we can provide an extraordinarily simple proof. In light of class field theory, this theorem tells us that every finite Abelian extension is contained within a certain ray class field; as we will see in Chapter 6, proving that any finite Abelian extension of a number field K is contained in some ray class field is one of the main difficulties in the proof of the Existence Theorem. The second application is a proof of the principal ideal theorem, which states that every ideal in a number field K becomes principal in its Hilbert class field. The existence of a finite extension in which every ideal of K becomes principal is a direct consequence of the finiteness of the ideal class group; what is not trivial at all, and requires the power of class field theory, is the fact that the Hilbert class field satisfies this condition. The last application is a characterization of the primes which can be written in the form $x^2 + ny^2$ for all positive integer n. Some particular cases of this problem are classical results and had already been studied by Fermat, Euler, Legendre and Gauss, among others, but a general solution valid for all positive integer n requires the use of class field theory. Of course, there are many other applications of class field theory which we do not cover in this thesis, such as the higher reciprocity laws or a derivation of the Chebotarev density theorem from the generalized Dirichlet density theorem.

The sources used for each section are indicated at the beginning of the section.

This thesis aimed to be self-contained. However, unluckily this is not completely the case, since at a certain point the proof which we give of the global Reciprocity Law relies on the explicit description of the local Artin map for cyclotomic extensions of $\mathbb{Q}_p$. In the ramified case, this description is not provided by the theory developed in Chapter 3, where the existence of the local Artin map is proved in a non-constructive way. If this thesis were to be expanded, a new chapter on Lubin-Tate theory would amend this fault. For the interested reader, this theory is exposed in [Mil13, Chapter 1]. Apart from this point, and the omission of the proofs in the first sections of Chapter 1, which deal with a theory which is required but which falls out of the topic of this thesis, we can say that the thesis is self-contained. For those looking for proofs of the

results on group cohomology and homology, reference sources might be [Ser79, Chapter 7] and [Mil13, Chapter 2].

Regarding the prerequisites, this thesis assumes that the reader is familiar with the theory of field extensions and Galois theory (including infinite Galois theory), on the one side, and with the basic notions about number fields which are usually encountered in any introductory course to algebraic number theory, on the other side. For those wanting to introduce themselves in these two areas, good references are [Mil17b] and [Sam70], respectively. Nevertheless, for the reader's convenience, two particular topics in Galois theory and basic algebraic number theory, namely Kummer theory and the theory of orders in quadratic number fields, are concisely covered in the appendices, as they are sometimes omitted in introductory courses to these subjects.

Chapter 1

Galois Cohomology

In this chapter G will always denote a group.

1.1 G-modules

References: [Mil13]

Definition 1.1.1. A *G-module* is an Abelian group M together with an action of G on M:

$$\begin{aligned} G \times M &\to M \\ (g, m) &\mapsto gm \end{aligned}$$

satisfying

$$g(m + m') = gm + gm' \quad \forall g \in G, \forall m, m' \in M\,.$$

Let $\mathbb{Z}[G]$ be the ring obtained by taking the free Abelian group $\bigoplus_{g \in G} \mathbb{Z} \cdot g$ and defining multiplication in the following way:

$$\left(\sum_i n_i g_i\right)\left(\sum_j n_j g'_j\right) = \sum_{i,j} n_i n'_j (g_i g'_j)$$

(all the sums are over a finite number of elements). Then we may also consider a G-module as a module over the ring $\mathbb{Z}[G]$.

Definition 1.1.2. A *homomorphism of G-modules* or *G-homomorphism* is a map $\alpha : M \to N$, where both M and N are G-modules, such that:

1. $\alpha(m + m') = \alpha(m) + \alpha(m') \quad \forall m, m' \in M$.
2. $\alpha(gm) = g\alpha(m) \quad \forall g \in G, \forall m \in M$.

Note that a homomorphism of G-modules is also a homomorphism of $\mathbb{Z}[G]$-modules, so that the category of G-modules (which we will denote by Mod_G) is isomorphic to that of $\mathbb{Z}[G]$-modules.

Note that, given G-modules M and N, the set of homomorphisms of G-modules from M to N, which we will denote by $\mathrm{Hom}_G(M,N)$, has a structure of Abelian group with the sum defined in the natural way. It can also be provided with a structure of G-module by defining an action of G on $\mathrm{Hom}_G(M,N)$ as:

$$g\varphi(m) = g\varphi(g^{-1}m)) \quad \text{for all } \varphi \in \mathrm{Hom}_G(M,N) \text{ and for all } g \in G,\ m \in M.$$

Let G be a group, let H be a subgroup of G and let M be an H-module. Then we define $\mathrm{Ind}_H^G(M)$ as the set of maps $\varphi : G \to M$ satisfying $\varphi(hg) = h\varphi(g)$ for all $h \in H$ and for all $g \in G$. We define a sum in $\mathrm{Ind}_H^G(M)$ in the natural way and we define an action of G on $\mathrm{Ind}_H^G(M)$ by

$$(g\varphi)(x) = \varphi(xg) \quad \text{for all } \varphi \in \mathrm{Ind}_H^G(M) \text{ and for all } g \in G.$$

It is easy to check that, with these operations, $\mathrm{Ind}_H^G(M)$ is a G-module.

Given a homomormorphism of H-modules $\alpha : M \to M'$, it is easy to check that the map

$$\begin{aligned} \tilde{\alpha} : \mathrm{Ind}_H^G(M) &\to \mathrm{Ind}_H^G(M') \\ \varphi &\mapsto \alpha \circ \varphi \end{aligned}$$

is a homomorphism of G-modules. It is straightforward that $\mathrm{Ind}_H^G : \mathrm{Mod}_H \to \mathrm{Mod}_G$ sending M to $\mathrm{Ind}_H^G(M)$ and $\alpha : M \to M'$ to $\tilde{\alpha} : \mathrm{Ind}_H^G(M) \to \mathrm{Ind}_H^G(M')$ is a covariant functor. Moreover, it can be proved that the functor Ind_H^G is exact.

For $H = \{1\}$, we will write $\mathrm{Ind}^G(M)$ for $\mathrm{Ind}_H^G(M)$.

Definition 1.1.3. A G-module M is *induced* if $M \simeq \mathrm{Ind}^G(M_0)$ for some Abelian group M_0.

The tensor product (with respect to $\mathbb{Z}$) of two G-modules M and N is again a G-module with the action

$$g(m \otimes n) = gm \otimes gn \quad \text{for all } g \in G \text{ and for all } m \in M,\ n \in N.$$

All tensor products will be taken with respect to $\mathbb{Z}$, so that we will not usually specify it.

It can be proved that, if G is a finite group, then a G-module M is induced if and only if it is isomorphic (as a G-module) to $\mathbb{Z}[G] \otimes N$ for some G-module N.

1.2 Cohomology via injective resolutions

References: [Mil13]

We say that a G-module I is *injective* if the functor $\mathrm{Hom}_G(\cdot, I)$ is exact. Equivalently, a G-module I is injective if for any G-module M and for any G-submodule N of M, any G-homomorphism from N to I can be extended to a G-homomorphism from M to I.

An injective resolution of a G-module M is an exact sequence of G-modules

$$0 \longrightarrow M \longrightarrow I^0 \longrightarrow I^1 \longrightarrow I^2 \longrightarrow \cdots$$

in which the G-modules I^i are injective. It can be proved that, for any G-module, there always exists an injective resolution.

For a G-module M, we define:

$$M^G = \{m \in M \mid gm = m \text{ for all } g \in G\}.$$

It is easy to check that M^G is a subgroup of M as an Abelian group; it is called the *module of G-invariants of M*.

Note that, for any homomorphism of G-modules $\alpha : M \to N$, we have $\alpha(M^G) \subseteq N^G$, so that we may restrict it to the groups M^G and N^G. Thus, we can define a functor from Mod_G to Ab by sending any G-module M to M^G and restricting the homomorphisms of G-modules to these groups. This functor is left-exact, i.e. for any exact sequence of G-modules

$$0 \longrightarrow M \longrightarrow N \longrightarrow P \longrightarrow 0 \quad ,$$

the sequence

$$0 \longrightarrow M^G \longrightarrow N^G \longrightarrow P^G$$

is also exact.

Let M be a G-module and choose an injective resolution of M:

$$0 \longrightarrow M \longrightarrow I^0 \longrightarrow I^1 \longrightarrow I^2 \longrightarrow \cdots \quad .$$

Applying the left exact functor $(\cdot)^G$ on the sequence and removing M^G we get the complex

$$0 \xrightarrow{\mathrm{d}^{-1}} (I^0)^G \xrightarrow{\mathrm{d}^0} (I^1)^G \xrightarrow{\mathrm{d}^1} (I^2)^G \longrightarrow \cdots$$

which need no longer be exact.

For $r \geqslant 0$, the *r-th cohomology group of G with coefficients in M* is defined as

$$H^r(G, M) = \frac{\ker(\mathrm{d}^r)}{\mathrm{Im}(\mathrm{d}^{r-1})} \, .$$

It can be proved that, up to isomorphism, this definition does not depend on the choice of the injective resolution.

From the fact that the functor $(\cdot)^G$ is left-exact, it is straightforward that $H^0(G, M) = M^G$.

It is also straightforward that, if I is an injective G-module, then $H^r(G, I) = 0$ for $r > 0$.

Given a G-homomorphism $\alpha : M \to N$ and injective resolutions $M \to I^\bullet$ and $N \to J^\bullet$, we can extend α to a homomorphism of complexes of G-modules

$$\begin{array}{ccccccccc} M & \longrightarrow & I^0 & \longrightarrow & I^1 & \longrightarrow & I^2 & \longrightarrow & \cdots \\ \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \alpha^0} & & \downarrow{\scriptstyle \alpha^1} & & \downarrow{\scriptstyle \alpha^2} & & \\ N & \longrightarrow & J^0 & \longrightarrow & J^1 & \longrightarrow & J^2 & \longrightarrow & \cdots \end{array}$$

which induces homomorphisms in cohomology

$$H(\alpha^r) : H^r(G, M) \to H^r(G, N) \, .$$

It can be proved that the homomorphisms induced in cohomology do not depend on the choice of the extension $\alpha^\bullet$. This result applied to the identity map provides a well defined isomorphism for cohomology groups obtained from different injective resolutions.

A short exact sequence of G-modules

$$0 \longrightarrow M \longrightarrow M' \longrightarrow M'' \longrightarrow 0$$

gives rise canonically to a long exact sequence

$$0 \longrightarrow H^0(G,M) \longrightarrow H^0(G,M') \longrightarrow H^0(G,M'') \longrightarrow H^1(G,M) \longrightarrow \cdots .$$

Moreover, a homomorphism of short exact sequences induces a homomorphism between the corresponding long exact sequences with the homomorphisms induced in cohomology.

Let M be a G-module, let M_0 be M regarded as an Abelian group and let $M' = \mathrm{Ind}(M_0)$. We can embed M into M' by associating to each $m \in M$ the map $\varphi : G \to M_0$ sending any $g \in G$ to gm. Then, we get an exact sequence of G-modules

$$0 \longrightarrow M \longrightarrow M' \longrightarrow M'/M \longrightarrow 0 \tag{1.1}$$

in which M' is induced. Moreover, it can be proved that this exact sequence is split.

A product of G-modules $\prod_{i\in I} M_i$ is again a G-module with the action

$$g(m_i)_{i\in I} = (gm_i)_{i\in I} ,$$

and we have the following property:

$$H^r\left(G, \prod_{i\in I} M_i\right) = \prod_{i\in I} H^r(G, M_i) .$$

1.3 Cohomology via cochains

References: [Mil13]

Now we will give an explicit description of the cohomology groups. Given a G-module M, for $r \geqslant 0$, an *r-cochain with values in M* is a map $\varphi : G^r \to M$ (understanding that $G^0 = \{1\}$). The sum of r-cochains is defined in the natural way, and this clearly provides the set of r-cochains with values in M with a structure of Abelian group. We denote this group by $C^r(G,M)$. For each $r \geqslant 0$, we define a map

$$\mathrm{d}^r : C^r(G,M) \to C^{r+1}(G,M)$$

by

$$\mathrm{d}^r\varphi(g_1,\ldots,g_{r+1}) = g_1\varphi(g_2,\ldots,g_{r+1}) + \sum_{j=1}^{r}(-1)^j\varphi(g_1,\ldots,g_jg_{j+1},\ldots,g_{r+1}) + (-1)^{r+1}\varphi(g_1,\ldots,g_r)$$

for all $\varphi \in C^r(G,M)$ and for all $g_1,\ldots,g_{r+1} \in G$. It is straightforward that these maps define a complex

$$C^0(G,M) \xrightarrow{\mathrm{d}^0} C^1(G,M) \xrightarrow{\mathrm{d}^1} C^2(G,M) \longrightarrow \cdots ,$$

i.e. $\mathrm{d}^{r+1} \circ \mathrm{d}^r = 0$ for all $r \geqslant 0$. We define the groups $Z^r(G, M) = \ker \mathrm{d}^r$ and $B^r(G, M) = \operatorname{Im} \mathrm{d}^{r-1}$, whose elements are called r-cocycles and r-coboundaries, respectively (for convenience we can define d^{-1} as the trivial map $0 \to C^0(G, M)$).

Then, we have

$$H^r(G, M) \simeq \frac{Z^r(G, M)}{B^r(G, M)}\,.$$

Given a short exact sequence of G-modules

$$0 \longrightarrow M \xrightarrow{\alpha} M' \xrightarrow{\beta} M'' \longrightarrow 0\,,$$

we can now give an explicit description of the maps in the induced long exact sequence

$$0 \longrightarrow H^0(G, M) \longrightarrow H^0(G, M') \longrightarrow H^0(G, M'') \longrightarrow H^1(G, M) \longrightarrow \cdots\,.$$

The maps

$$H^r(G, M) \to H^r(G, M')$$

and

$$H^r(G, M') \to H^r(G, M'')$$

are the natural ones, i.e. the maps induced by $\varphi \mapsto \alpha \circ \varphi$ and $\varphi \mapsto \beta \circ \varphi$, respectively. Now, let φ be an r-cocycle with values in M''; take some $\tilde{\varphi} \in C^r(G, M')$ such that $\beta \circ \tilde{\varphi} = \varphi$; then $\beta \circ \mathrm{d}^r \tilde{\varphi} = \mathrm{d}^r(\beta \circ \tilde{\varphi}) = 0$, which shows that $\mathrm{d}^r \tilde{\varphi}$ takes values in M, and it is easily seen that it is a cocycle. The map $\varphi \mapsto \mathrm{d}^r \tilde{\varphi}$ just described induces the homomorphism

$$H^r(G, M'') \to H^{r+1}(G, M)$$

in the long exact sequence.

1.4 Maps between cohomology groups

References: [Mil13]

Let M be a G-module and let M' be a G'-module (where G' is a group). Then, a pair of homomorphisms

$$\begin{aligned} \alpha &: G' \to G \\ \beta &: M \to M' \end{aligned}$$

are said to be *compatible* if

$$\beta(\alpha(g')m) = g'\beta(m) \quad \text{for all } g' \in G' \text{ and } m \in M.$$

In this case, the homomorphisms

$$\begin{aligned} C^r(G, M) &\to C^r(G', M') \\ \varphi &\mapsto \beta \circ \varphi \circ \alpha^r \end{aligned}$$

define a homomorphism of complexes $C^\bullet(G,M) \to C^\bullet(G',M')$ and hence they induce homomorphisms in cohomology

$$H^r(G,M) \to H^r(G',M')\,.$$

For example, if H is a subgroup of G and M is a G-module, the inclusion $H \hookrightarrow G$ and the identity map $M \to M$ are compatible. In this case, the induced homomorphisms

$$H^r(G,M) \to H^r(H,M)$$

are called *restriction maps* and are denoted by Res.

Another important example of compatible homomorphisms is the case of the quotient map $G \to G/H$ and the inclusion map $M^H \hookrightarrow M$, where H is a normal subgroup of G and M is a G-module. In this case, the induced homomorphisms

$$H^r(G/H, M^H) \to H^r(G,M)$$

are called *inflation maps* and are denoted by Inf.

Proposition 1.4.1. (Shapiro's lemma) Let H be a subgroup of G and let N be an H-module. Then, the inclusion $H \hookrightarrow G$ and the homomorphism

$$\begin{aligned} \mathrm{Ind}_H^G(N) &\to N \\ \varphi &\mapsto \varphi(1_G) \end{aligned}$$

are compatible and provide canonical isomorphisms

$$H^r(G, \mathrm{Ind}_H^G(N)) \xrightarrow{\simeq} H^r(H,N)$$

for all $r \geqslant 0$.

Remark 1. Because of the previous proposition, for an induced G-module $M = \mathrm{Ind}^G(M_0)$ we have

$$H^r(G,M) = H^r(G, \mathrm{Ind}_{\{1\}}^G(M_0)) = H^r(\{1\}, M_0) = 0$$

for all $r > 0$.

We also have the following lemma related to compatible maps, which we will require in future chapters. We will give the proof of the lemma to present an example of a method which is known as dimension shifting.

Lemma 1.4.2. For all $g_0 \in G$, the homomorphism $\alpha : G \to G$ defined by $g \mapsto g_0 g g_0^{-1}$ and the homomorphism $\beta : M \to M$ defined by $m \mapsto g_0^{-1} m$ are compatible and for all $r \geqslant 0$ the induced homomorphism

$$H^r(G,M) \to H^r(G,M)$$

is the identity map.

Proof. The fact that α and β are compatible is straightforward. Now, we prove by induction on r that the induced homomorphisms

$$H^r(G,M) \to H^r(G,M)$$

are the identity map. All 0-cocycles $\varphi : \{1\} \to M$ must have image in M^G because of the condition $\mathrm{d}^0\varphi = 0$ (in fact, we can obviously identify $C^0(G,M)$ with M and $Z^0(G,M)$ with M^G). Therefore, the induced map

$$\begin{aligned} M^G &\to M^G \\ m &\mapsto g_0^{-1} m \end{aligned}$$

is clearly the identity map.

Now, assume that it is true for r and let us prove it for $r+1$. We know that there is an exact sequence of G-modules

$$0 \longrightarrow M \longrightarrow M' \longrightarrow M'' \longrightarrow 0$$

such that M' is induced. Then, we get a diagram

$$\begin{array}{ccccccc} H^{r-1}(G,M') & \longrightarrow & H^{r-1}(G,M'') & \longrightarrow & H^r(G,M) & \longrightarrow & H^r(G,M')=0 \\ \downarrow & & \downarrow & & \downarrow & & \\ H^{r-1}(G,M') & \longrightarrow & H^{r-1}(G,M'') & \longrightarrow & H^r(G,M) & \longrightarrow & H^r(G,M')=0 \end{array}$$

where the vertical arrows are the maps induced by the corresponding pairs α, β. It is easy to see that the diagram commutes. Since, by induction, the second vertical arrow is the identity, so is the third. □

Now, let H be a subgroup of G of finite index and let M be a G-module. Let S be a set of left coset representatives for H in G. Then, we define the map

$$\begin{aligned} \mathrm{Nm}_{G/H} : M^H &\to M^G \\ m &\mapsto \sum_{s\in S} sm\,, \end{aligned}$$

which does not depend on the choice of S. When $H=\{1\}$, we will simply write Nm_G. For $r \geqslant 0$, we define the *corestriction maps* as the homomorphisms obtained as the composite

$$H^r(H,M) \to H^r(G, \mathrm{Ind}_H^G(M)) \to H^r(G,M)\,,$$

where the first arrow is the isomorphism from Shapiro's lemma and the second arrow is induced by the homomorphism $\mathrm{Ind}_H^G(M) \to M$ defined by $\varphi \mapsto \sum_{s\in S} s\varphi(s^{-1})$. It is a straightforward calculation to check that the diagram

$$\begin{array}{ccc} H^0(H,M) & \xrightarrow{\simeq} & M^H \\ \downarrow{\scriptstyle \mathrm{Cor}} & & \downarrow{\scriptstyle \mathrm{Nm}_{G/H}} \\ H^0(G,M) & \xrightarrow{\simeq} & M^G \end{array} \tag{1.2}$$

commutes.

The restriction, inflation and corestriction maps induce morphisms between the long exact sequences obtained from a short exact sequence of G-modules; i.e. if

$$0 \longrightarrow M \longrightarrow M' \longrightarrow M'' \longrightarrow 0$$

is a short exact sequence of G-modules, and H is a subgroup of G, we have, for example, the commutative diagram

$$\begin{array}{ccccccccccc} 0 & \longrightarrow & H^0(G,M) & \longrightarrow & H^0(G,M') & \longrightarrow & H^0(G,M'') & \longrightarrow & H^1(G,M) & \longrightarrow & \cdots \\ & & \downarrow{\scriptstyle \mathrm{Res}} & & \downarrow{\scriptstyle \mathrm{Res}} & & \downarrow{\scriptstyle \mathrm{Res}} & & \downarrow{\scriptstyle \mathrm{Res}} & & \\ 0 & \longrightarrow & H^0(H,M) & \longrightarrow & H^0(H,M') & \longrightarrow & H^0(H,M'') & \longrightarrow & H^1(H,M) & \longrightarrow & \cdots \end{array}$$

.

We have the following proposition related to the restriction and corestriction maps:

Proposition 1.4.3. Let H be a subgroup of G of finite index. Then, the composite $\mathrm{Cor} \circ \mathrm{Res}$ is multiplication by $[G : H]$.

Corollary 1.4.4. Assume that G is finite of order n, and let M be a G-module. Then, $nH^r(G, M) = 0$ for all $r > 0$.

Corollary 1.4.5. If G is finite and G_p is a p-Sylow subgroup (where p is a prime number), then for any G-module M the restriction map

$$\mathrm{Res} : H^r(G, M) \to H^r(G_p, M)$$

is injective on the p-primary component of G (i.e. the subgroup comprised of the elements of order a power of p).

Another important result is the inflation-restriction sequence:

Proposition 1.4.6. Let H be a normal subgroup of G and let M be a G-module. Then, if $H^i(H, M) = 0$ for all $0 < i < r$, the sequence

$$0 \longrightarrow H^r(G/H, M^H) \xrightarrow{\mathrm{Inf}} H^r(G, M) \xrightarrow{\mathrm{Res}} H^0(H, M)$$

is exact.

1.5 Cup-products

References: [Mil13]

Proposition 1.5.1. There exists a unique family of bi-additive maps

$$\begin{aligned} H^r(G, M) \times H^s(G, N) &\to H^{r+s}(G, M \otimes N) \\ (m, n) &\mapsto m \cup n \end{aligned}$$

defined for all G-modules M, N and for all $r, s \geqslant 0$ satisfying that:

1. When both sides are regarded as bi-functors in (M, N), then the maps provide a morphism of bi-functors.
2. For $r = s = 0$, the map is
$$\begin{aligned} M^G \times N^G &\to (M \otimes N)^G \\ (m, n) &\mapsto m \otimes n\,. \end{aligned}$$
3. If
$$0 \longrightarrow M \longrightarrow M' \longrightarrow M'' \longrightarrow 0$$
is exact and so is
$$0 \longrightarrow M \otimes N \longrightarrow M' \otimes N \longrightarrow M'' \otimes N \longrightarrow 0\,,$$

then

$$(\delta m'') \cup n = \delta(m'' \cup n)$$

for all $m'' \in H^r(G, M'')$ and for all $n \in H^s(G, N)$, with $r, s \geqslant 0$, where δ is in each case the connecting map $H^r(G, M'') \to H^{r+1}(G, M)$ or $H^{r+s}(G, M'' \otimes N) \to H^{r+s+1}(G, M \otimes N)$.

4. If

$$0 \longrightarrow N \longrightarrow N' \longrightarrow N'' \longrightarrow 0$$

is exact and so is

$$0 \longrightarrow M \otimes N \longrightarrow M \otimes N' \longrightarrow M \otimes N'' \longrightarrow 0 \quad ,$$

then

$$m \cup (\delta n'') = (-1)^r \delta(m \cup n'')$$

for all $m \in H^r(G, M)$ and for all $n'' \in H^s(G, N'')$, with $r, s \geqslant 0$, where δ is in each case the connecting map $H^r(G, N'') \to H^{r+1}(G, N)$ or $H^{r+s}(G, M \otimes N'') \to H^{r+s+1}(G, M \otimes N)$.

The binary operation from the previous proposition is called cup-product. It can be given an explicit description in terms of cochains. If $\varphi \in Z^r(G, M)$ is an r-cocycle representing an element $m \in H^r(G, M)$ and $\psi \in Z^s(G, N)$ is an s-cocycle representing an element $n \in H^s(G, N)$, then $m \cup n$ is represented by the cocycle defined by

$$(g_1, \ldots, g_{r+s}) \mapsto \varphi(g_1, \ldots, g_r) \otimes g_1 \cdots g_r \psi(g_{r+1}, \ldots, g_{r+s}) \, .$$

Let M, N and P be G-modules. Then, the cup-product satisfies the following properties:

1. For any $x \in H^r(G, M)$, $y \in H^s(G, N)$ and $z \in H^t(G, P)$,

$$(x \cup y) \cup z = x \cup (y \cup z)$$

in $H^{r+s+t}(G, M \otimes N \otimes P)$.

2. For any $x \in H^r(G, M)$ and $y \in H^s(G, N)$,

$$x \cup y = (-1)^{rs} y \cup x \, .$$

3. For any $x \in H^r(G, M)$ and $y \in H^s(G, N)$,

$$\mathrm{Res}(x \cup y) = \mathrm{Res}(x) \cup \mathrm{Res}(y) \, ,$$

where the maps Res correspond to a certain subgroup H of G.

4. For any $x \in H^r(G, M)$ and $y \in H^s(G, N)$,

$$\mathrm{Cor}(x \cup \mathrm{Res}(y)) = \mathrm{Cor}(x) \cup y \, ,$$

where the maps Res and Cor correspond to a certain subgroup H of G of finite index.

1.6 Homology via projective resolutions

References: [Mil13]

We say that a G-module P is *projective* if the functor $\mathrm{Hom}_G(P, \cdot)$ is exact. Equivalently, a G-module P is projective if for any G-module M, any G-homomorphism from P to a quotient of M can be lifted to a homomorphism from P to M. In particular, we easily see that any free $\mathbb{Z}[G]$-module is projective.

A projective resolution of a G-module M is an exact sequence of G-modules

$$\cdots \longrightarrow P_2 \longrightarrow P_1 \longrightarrow P_1 \longrightarrow M \longrightarrow 0$$

in which the G-modules P_i are all projective. It can be proved that, for any G-module, there always exist a projective resolution.

For a G-module M, we define

$$M_G = M/I_G M\,,$$

where I_G is the kernel of the augmentation map

$$\begin{aligned} \epsilon : \mathbb{Z}[G] &\to \mathbb{Z} \\ \sum_{g\in G} n_g g &\mapsto \sum_{g\in G} n_g \end{aligned}$$

It is easy to see that M_G is the largest quotient of M on which G acts trivially; it is called the *module of G-coinvariants of M*.

Observe that, given a G-homomorphism $\alpha : M \to N$, we have $\alpha(I_G M) \subseteq I_G N$, so that α induces a homomorphism of Abelian groups $M_G \to N_G$. Hence, we can define a functor from Mod_G to Ab by sending any G-module M to M_G and any G-homomorphism to the corresponding induced homomorphism. Moreover, it can be seen that this functor is right-exact, i.e. for any exact sequence of G-modules

$$0 \longrightarrow M \longrightarrow N \longrightarrow P \longrightarrow 0\,,$$

the sequence

$$M_G \longrightarrow N_G \longrightarrow P_G \longrightarrow 0$$

is also exact.

Let M be a G-module and choose projective resolution of M:

$$\cdots \longrightarrow P_2 \longrightarrow P_1 \longrightarrow P_0 \longrightarrow M \longrightarrow 0\,.$$

Applying the right-exact functor $(\cdot)_G$ on the sequence and removing M_G we get the complex

$$\cdots \longrightarrow (P_2)_G \xrightarrow{\mathrm{d}_2} (P_1)_G \xrightarrow{\mathrm{d}_1} (P_0)_G \xrightarrow{\mathrm{d}_0} 0$$

which need no longer be exact.

For $r \geqslant 0$, the *r-th homology group of G with coefficients in M* is defined as

$$H_r(G, M) = \frac{\ker(\mathrm{d}_r)}{\mathrm{Im}(\mathrm{d}_{r+1})} .$$

It can be proved that, up to isomorphism, this definition does not depend on the choice of the projective resolution.

From the fact that the functor $(\cdot)_G$ is right-exact, it is straightforward that $H_0(G, M) = M_G$.

It is also straightforward that, if P is a projective G-module, then $H_r(G, P) = 0$ for $r > 0$.

Given a G-homomorphism $\alpha : M \to N$ and projective resolutions $P_\bullet \to M$ and $Q_\bullet \to N$, we can extend α to a homomorphism of complexes of G-modules

$$\begin{array}{ccccccccc}
\cdots & \longrightarrow & P_2 & \longrightarrow & P_1 & \longrightarrow & P_0 & \longrightarrow & M \\
 & & \downarrow{\scriptstyle \alpha_2} & & \downarrow{\scriptstyle \alpha_1} & & \downarrow{\scriptstyle \alpha_0} & & \downarrow{\scriptstyle \alpha} \\
\cdots & \longrightarrow & Q_2 & \longrightarrow & Q_1 & \longrightarrow & Q_0 & \longrightarrow & N
\end{array}$$

which induces homomorphisms in homology

$$H(\alpha_r) : H_r(G, M) \to H_r(G, N) .$$

It can be proved that the homomorphisms induced in homology do not depend on the choice of the extension $\alpha_\bullet$. This result applied to the identity map provides a well defined isomorphism for homology groups obtained from different projective resolutions.

A short exact sequence of G-modules

$$0 \longrightarrow M \longrightarrow M' \longrightarrow M'' \longrightarrow 0$$

gives rise canonically to a long exact sequence

$$\cdots \longrightarrow H_1(G, M'') \longrightarrow H_0(G, M) \longrightarrow H_0(G, M') \longrightarrow H_0(G, M'') \longrightarrow 0 .$$

Moreover, a homomorphism of short exact sequences induces a homomorphism between the corresponding long exact sequences with the homomorphisms induced in homology.

Proposition 1.6.1. If M is an induced G-module, then $H_r(G, M) = 0$ for all $r > 0$.

1.7 Homology via chains

References: [Ser79]

We now give an explicit description of the homology groups. Let M be a G-module. For $r \geqslant 0$, an *r-chain with values in M* a map $G^r \to M$ which takes the value zero at all except for finitely many elements of G^r. We define $C_r(G, M)$ as the Abelian group having as elements the r-chains with values in M and with the sum defined in the natural way. We define maps

$$\mathrm{d}_r : C_r(G, M) \to C_{r-1}(G, M)$$

for $r > 0$ by

$$\mathrm{d}_r\varphi(g_1,\dots,g_{r-1}) = \sum_{g\in G} g^{-1}\varphi(g,g_1,\dots,g_{r-1}) + \\ + \sum_{j=1}^{r-1}(-1)^j \sum_{g\in G}\varphi(g_1,\dots,g_jg,g^{-1},g_{j+1},\dots,g_{r-1}) + (-1)^r \sum_{g\in G}\varphi(g_1,\dots,g_{r-1},g)$$

and, for $r = 0$, as the trivial map

$$\mathrm{d}_0 : C_0(G,M) \to 0\,.$$

It is straightforward that with these maps we get a complex $C_\bullet(G,M)$, i.e. that $\mathrm{d}_{r-1}\circ\mathrm{d}_r = 0$ for all $r > 0$. We define the group of r-cycles as $Z_r(G,M) = \ker \mathrm{d}_r$ and the group of r-boundaries as $B_r(G,M) = \operatorname{Im}\mathrm{d}_{r+1}$. Then, we have

$$H_r(G,M) \simeq \frac{Z_r(G,M)}{B_r(G,M)}\,.$$

As in cohomology, using this description of the homology groups we also get an explicit description of the homomorphisms appearing in the long exact sequence of homology groups coming from an exact sequence of G-modules. This descrition is completely analogous to the one we gave for the case of cohomology.

1.8 Cohomology of profinite groups

References: [Mil13]

Through this section G will be a profinite group, that is, a topological group which is the projective limit of finite groups, each of them with the discrete topology. A profinite group is compact, Hausdorff and the open normal subgroups form a fundamental system of neighborhoods of 1. It will usually be the Galois group of some infinite Galois extension endowed with the Krull topology.

Definition 1.8.1. A *discrete G-module* is a G-module M endowed with the discrete topology such that the map

$$G \times M \to M$$

defined by the action of G on M is continuous.

Again, cohomology groups can be defined for any discrete G-module using injective resolutions in the same way as in section 1.2. However, we will go directly to the definition of the cohomology groups in terms of cochains.

Let M be a discrete G-module. Then, for $r \geqslant 0$ we define $C^r_{\mathrm{cts}}(G,M)$ as the set of continuous r-cochains with values in M, i.e. the set of continuous maps $G^r \to M$. Since M is endowed with the discrete topology, the continuity condition is simply that the preimage of any element of M be an open subset of G^r. Then, it is easy to see that $C^r_{\mathrm{cts}}(G,M)$ is in fact a subgroup of $C^r(G,M)$, and that the maps d^r defined in section 1.3 restrict to maps

$$C^r_{\mathrm{cts}}(G,M) \to C^{r+1}_{\mathrm{cts}}(G,M)\,.$$

We define cohomology groups using the complex $C^\bullet_{\mathrm{cts}}(G,M)$:

$$\mathrm{Hom}^r_{\mathrm{cts}}(G,M) = \frac{Z^r_{\mathrm{cts}}(G,M)}{B^r_{\mathrm{cts}}(G,M)} \quad \text{for } r \geqslant 0,$$

where $Z^r_{\mathrm{cts}}(G,M) = \ker \mathrm{d}^r$ and $B^r_{\mathrm{cts}}(G,M) = \operatorname{Im} \mathrm{d}^{r-1}$.

Let M be a discrete G-module and let M' be a discrete G'-module (where G' is also a profinite group). Then, a pair of continuous homomorphisms

$$\begin{aligned} \alpha &: G' \to G \\ \beta &: M \to M' \end{aligned}$$

are *compatible* if

$$\beta(\alpha(g')m) = g\beta(m) \quad \text{for all } g' \in G' \text{ and for all } m \in M.$$

In this case, it is straightforward that the homomorphisms

$$\begin{aligned} C^r(G,M) &\to C^r(G',M') \\ \varphi &\mapsto \beta \circ \varphi \circ \alpha^r \end{aligned}$$

define a morphism of complexes $C^\bullet_{\mathrm{cts}}(G,M) \to C^\bullet_{\mathrm{cts}}(G',M')$ and hence they induce homomorphisms in cohomology

$$H^r_{\mathrm{cts}}(G,M) \to H^r_{\mathrm{cts}}(G',M')\,.$$

If H is a closed subgroup of G, then H is a profinite group. The inclusion $H \hookrightarrow G$ and the identity map on M are compatible and provide the restricion homomorphisms

$$\mathrm{Res} : H^r_{\mathrm{cts}}(G,M) \to H^r_{\mathrm{cts}}(H,M)\,.$$

If H is a closed normal subgroup of G, then G/H is also a profinite group. The projection $G \to G/H$ and the inclusion $M^H \hookrightarrow M$ are compatible and provide the inflation homomorphisms

$$\mathrm{Inf} : H^r_{\mathrm{cts}}(G/H, M^H) \to H^r_{\mathrm{cts}}(G,M)\,.$$

Now, let us temporarily use the notation Inf to denote also the maps

$$C^r_{\mathrm{cts}}(G/H, M^H) \to C^r_{\mathrm{cts}}(G,M)$$

provided by the compatible maps $G \to G/H$ and $M^H \hookrightarrow M$. Observe that, since G is compact, any open subgroup H of G is closed and has finite index in G; in particular, if H is an open normal subgroup of G, then $C^r_{\mathrm{cts}}(G/H, M^H) = C^r(G/H, M^H)$. For each $r \geqslant 0$, the groups $C^r(G/H, M^H)$ with H an open normal subgroup of G, indexed by H with the order opposite to inclusion, together with the maps

$$\mathrm{Inf} : C^r(G/H, M^H) \to C^r(G/H', M^{H'})$$

defined for the pairs of open normal subgroups H and H' of G with $H \supset H'$, clearly form a direct system. Moreover, the maps

$$\mathrm{Inf} : C^r(G/H, M^H) \to C^r_{\mathrm{cts}}(G,M)$$

are clearly compatible with the maps in the direct system, and are clearly injective, so that we get an injective homomorphism

$$\varinjlim C^r(G/H, M^H) \to C^r_{\mathrm{cts}}(G,M)\,.$$

In fact, we get a morphism of complexes

$$\varinjlim C^\bullet(G/H, M^H) \to C^\bullet_{\text{cts}}(G, M)\,.$$

Let $\varphi : G^r \to M$ be a continuous r-cochain. Since G^r is compact (because G is profinite) the image of φ is also compact, and, since M is endowed with the discrete topology, it is finite. For each $m \in M$, the map

$$\begin{aligned} G &\to M \\ g &\mapsto gm \end{aligned}$$

is continuous, so that the preimage of m by this map, i.e. the elements of G fixing m, is an open subgroup of G. Since for a profinite group the open normal subgroups form a fundamental system of neighborhoods of 1, there is some open normal subgroup K_m fixing m. If we define $K = \bigcap_{m\in\varphi(G^r)} K_m$, we get an open normal subgroup such that $\varphi(G^r) \subseteq M^K$. On the other hand, for each $m \in \varphi(G^r)$, the preimage $\varphi^{-1}(m)$ is an open subset of G^r, so that, taking into account again that the open normal subgroups of G form a fundamental system of neighborhoods of 1, for each $x \in \varphi^{-1}(m)$, there exists some open normal subgroup H_x such that $x(H_x)^r \subseteq \varphi^{-1}(m)$. The sets $x(H_x)^r$ with $x \in \varphi^{-1}(m)$ clearly form an open cover of $\varphi^{-1}(m)$. Since this subset of G^r is closed and consequently compact, there exist some $x_1, \ldots, x_{j_m}$ such that $\varphi^{-1}(m) = \bigcup_{i=1}^{j_m} x_i(H_{x_i})^r$, so that, defining $H_m = \bigcap_{i=1}^{j_m} H_{x_i}$, we get an open normal subgroup such that $x(H_m)^r \subseteq \varphi^{-1}(m)$ for all $x \in \varphi^{-1}(m)$. Taking $H = \bigcap_{m\in\varphi(G^r)} H_m$, we get an open normal subgroup of G such that φ factors through $(G/H)^r$. Finally, if we define $H' = H \cap K$, we see that φ comes by inflation from an element of $C^r(G/H', M^{H'})$.

Thus, the previous morphism of complexes

$$\varinjlim C^\bullet(G/H, M^H) \to C^\bullet_{\text{cts}}(G, M)\,.$$

is in fact an isomorphism.

Proposition 1.8.2. Let M be a discrete G-module. Then, the maps $\text{Inf} : H^r(G/H, M^H) \to H^r_{\text{cts}}(G, M)$, where H runs through the open normal subgroups of G, provide natural isomorphisms

$$\varinjlim H^r(G/H, M^H) \simeq H^r_{\text{cts}}(G, M)$$

for all $r \geqslant 0$, where the direct limit is taken through the open normal subgroups H of G, with order the opposite of inclusion and homomorphisms $\text{Inf} : H^r(G/H, M^H) \to H^r(G/H', M^{H'})$.

Proof. For every complex $C^\bullet$, the groups $Z^r(C^\bullet)$, $B^r(C^\bullet)$ and $H^r(C^\bullet)$ can be defined in exactly the same way we did for the particular case of the complex $C^\bullet_{\text{cts}}(G, M)$. The isomorphism of complexes

$$\varinjlim C^\bullet(G/H, M^H) \to C^\bullet_{\text{cts}}(G, M)\,.$$

found in the previous discussion shows that the inflation maps provide isomorphisms

$$H^r\left(\varinjlim C^\bullet\left(G/H, M^H\right)\right) \simeq H^r\left(C^\bullet_{\text{cts}}\left(G, M\right)\right) = H^r_{\text{cts}}\left(G, M\right)$$

for all $r \geqslant 0$. Then, the desired result follows from the sequence of natural isomorphisms

$$H^r\left(\varinjlim C^\bullet\left(G/H, M^H\right)\right) \simeq \frac{Z^r\left(\varinjlim C^\bullet\left(G/H, M^H\right)\right)}{B^r\left(\varinjlim C^\bullet\left(G/H, M^H\right)\right)} \simeq \frac{\varinjlim Z^r\left(C^\bullet\left(G/H, M^H\right)\right)}{\varinjlim B^r\left(C^\bullet\left(G/H, M^H\right)\right)} \simeq$$

$$\simeq \varinjlim \frac{Z^r\left(C^\bullet\left(G/H, M^H\right)\right)}{B^r\left(C^\bullet\left(G/H, M^H\right)\right)} \simeq \varinjlim H^r\left(C^\bullet\left(G/H, M^H\right)\right) \simeq \varinjlim H^r\left(G/H, M^H\right)\,.$$

□

From now on (including the following chapters) for profinite groups we will always use the cohomology groups obtained from continuous cochains, so that we will omit the subscript 'cts'.

The previous proposition allows to extend some results of cohomology valid when G is finite to the case when G is profinite. For example, we get the following corollary:

Corollary 1.8.3. Let M be a discrete G-module. Then, the groups $H^r(G, M)$ are torsion for all $r > 0$.

Proof. This is a consequence of Corollary 1.4.4 and the previous proposition. □

Proposition 1.8.4. Let $\{M_i\}_{i\in I}$ be a direct system of discrete G-modules ordered by inclusion and let $M = \varinjlim M_i$. Then, the natural homomorphisms

$$C^r(G, M_i) \to C^r(G, M)$$

provide a natural isomorphism

$$\varinjlim H^r(G, M_i) \to H^r(G, M)\,.$$

Proof. For each $r \geqslant 0$, the natural homomorphisms $C^r(G, M_i) \to C^r(G, M)$ mapping a cochain $\varphi \in C^r(G, M_i)$ to the composite of this cochain with the map $M_i \hookrightarrow M$ are clearly injective and are obviously compatible with the maps $C^r(G, M_i) \to C^r(G, M_j)$ defined in the same way whenever $i \leqslant j$. Then, we get injective homomorphisms

$$\varinjlim C^r(G, M_i) \to C^r(G, M)$$

and, in fact, a morphism of complexes

$$\varinjlim C^\bullet(G, M_i) \to C^\bullet(G, M)\,.$$

Since the image of any continuous r-cochain $\varphi \in C^r(G, M)$ is finite and the G-modules M_i form a directed set with order defined by inclusion, any continuous cochain can be thought of as taking values in some M_k, so that we see that the homomorphisms

$$\varinjlim C^r(G, M_i) \to C^r(G, M)$$

are surjective and therefore the morphism of complexes

$$\varinjlim C^\bullet(G, M_i) \to C^\bullet(G, M)\,.$$

is in fact an isomorphism. Now, we simply proceed as in Proposition 1.8.2. □

An important example of cohomology with profinite groups is the case of Galois groups of Galois extensions of fields L/K acting on some subgroup of L or $L^\times$.

Proposition 1.8.5. (Hilbert's theorem 90) Let L/K be a Galois extension of fields and let $G = \mathrm{Gal}(L/K)$. Then $H^1(G, L^\times) = 0$.

Proof. Because of Proposition 1.8.2, it suffices to prove the result whenever the extension L/K is finite.

Let $\varphi : G \to L^\times$ be a 1-cocycle. Define $g = \sum_{\tau\in G} \varphi(\tau)\tau : L \to L$. Because of Dedekind's lemma on the independence of characters applied to the characters $\tau : L^\times \to L^\times$ with $\tau \in G$, the homomorphism of K-vector spaces g is not zero, so that there is some $a \in L^\times$ such that

$$b = \sum_{\tau\in G} \varphi(\tau)\cdot\tau a \neq 0\,.$$

For this element and for all $\sigma \in G$ we have

$$\sigma b = \sum_{\tau\in G} \sigma\varphi(\tau)\cdot\sigma\tau a = \sum_{\tau\in G} \varphi(\sigma)^{-1}\varphi(\sigma\tau)\sigma\tau a = \varphi(\sigma)^{-1}b\,,$$

where we have used that, since φ is a 1-cocycle,

$$\varphi(\sigma\tau) = \sigma\varphi(\tau)\cdot\varphi(\sigma) \quad \text{for all } \sigma,\tau \in G.$$

Finally, from the fact that, for all $\sigma \in G$,

$$\varphi(\sigma) = \frac{b}{\sigma b} = \frac{\sigma\left(b^{-1}\right)}{b^{-1}}\,,$$

we see that φ is a 1-coboundary.

Since any 1-cocycle is a 1-coboundary, we deduce that $H^1(G, L^\times) = 0$. □

Proposition 1.8.6. Let L/K be a Galois extension of fields with Galois group $G = \mathrm{Gal}(L/K)$. Then, for all $r > 0$, it holds $H^r(G, L) = 0$.

Proof. Again, because of Proposition 1.8.2, it suffices to prove the result for finite Galois extensions.

Because of the normal basis theorem, there exists some $\alpha \in L$ such that the set $\{\sigma\alpha\}_{\sigma\in G}$ forms a basis of L as a K-vector space. Hence, we get an isomorphism of G-modules

$$\begin{aligned} K[G] &\to L \\ \sum_{\sigma\in G} a_\sigma\sigma &\mapsto \sum_{\sigma\in G} a_\sigma\sigma\alpha\,. \end{aligned}$$

Since $K[G] \simeq \mathrm{Ind}^G(K)$ is induced, we deduce that $H^r(G, L) \simeq H^r(G, K[G]) = 0$ for all $r > 0$. □

1.9 Tate cohomology

References: [Mil13]

In this section, unless otherwise stated, we will assume that G is finite.

For any G-module M, it is straightforward that $I_G M \subseteq \ker \mathrm{Nm}_G$ and $\mathrm{Nm}_G M \subseteq M^G$. Then, we get an exact sequence

$$0 \longrightarrow \ker \mathrm{Nm}_G/I_G M \longrightarrow M/I_G M \xrightarrow{\mathrm{Nm}_G} M^G \longrightarrow M^G/\mathrm{Nm}_G M \longrightarrow 0\,.$$

Observe that the groups in the middle are $H_0(G, M)$ and $H^0(G, M)$.

For a short exact sequence of G-modules

$$0 \longrightarrow M \longrightarrow M' \longrightarrow M'' \longrightarrow 0 \quad ,$$

it is straightforward that the diagram

$$\begin{array}{ccccccccc} H_1(G,M'') & \longrightarrow & H_0(G,M) & \longrightarrow & H_0(G,M') & \longrightarrow & H_0(G,M'') & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathrm{Nm}_G} & & \downarrow{\scriptstyle \mathrm{Nm}_G} & & \downarrow{\scriptstyle \mathrm{Nm}_G} & & \\ 0 & \longrightarrow & H^0(G,M) & \longrightarrow & H^0(G,M') & \longrightarrow & H^0(G,M'') & \longrightarrow & H^1(G,M) \end{array} \quad ,$$

where the rows are the homology and cohomology sequences induced by the short exact sequence, commutes. Then, by means of the extended snake lemma, we get an exact sequence

$$\cdots \to H_T^{r-1}(G,M'') \to H_T^r(G,M) \to H_T^r(G,M') \to H_T^r(G,M'') \to H_T^{r+1}(G,M) \to \cdots \quad ,$$

where we use the notation $H_T^r(G,\cdot)$ for the Tate cohomology groups, which, for a given G-module N, are defined as

$$H_T^r(G,N) = \begin{cases} H^r(G,N) & \text{if } r > 0 \\ N^G/\mathrm{Nm}_G N & \text{if } r = 0 \\ \ker \mathrm{Nm}_G / I_G N & \text{if } r = -1 \\ H_{-r-1}(G,N) & \text{if } r < -1 \end{cases} \quad .$$

If there is no confusion, we will sometimes omit the subscript 'T'.

Proposition 1.9.1. If M is an induced G-module, then $H_T^r(G,M) = 0$ for all $r \in \mathbb{Z}$.

Proof. For $r > 0$ this is the remark following Proposition 1.4.1 and, for $r < -1$, this is Proposition 1.6.1, so we need only prove the result in the cases $r = 0$ and $r = -1$.

Since G is finite and M is induced, we have $M \simeq \mathbb{Z}[G] \otimes N$ for some G-module N. Take any $x = \sum_{g\in G} g \otimes n_g \in \mathbb{Z}[G] \otimes N$. If it is fixed by G, then for all $h \in G$

$$\sum_{g\in G} g \otimes n_g = \sum_{g\in G} hg \otimes hn_g = \sum_{g\in G} g \otimes hn_{h^{-1}g} \,,$$

which shows that, for all $g, h \in G$, we have $n_g = hn_{h^{-1}g}$. Taking $g = h$, we get that $n_g = gn_e$ for all $g \in G$, where e denotes the identity element of G, and, therefore, $x = \mathrm{Nm}_G(e \otimes n_e)$. We conclude that $M^G = \mathrm{Nm}_G M$ and consequently $H_T^0(G,M) = 0$.

Now, take again some $x = \sum_g g \otimes n_g \in \mathbb{Z}[G] \otimes N$ and assume that $\mathrm{Nm}_G(x) = 0$, so that

$$0 = \sum_{h\in G}\sum_{g\in G} hg \otimes hn_g = \sum_{h\in G}\sum_{g\in G} h(e \otimes g^{-1}n_g) \,.$$

Therefore, we have $\sum_{g\in G} g^{-1}n_g = 0$ and

$$x = \sum_{g\in G} g \otimes n_g - \sum_{g\in G} e \otimes g^{-1}n_g = \sum_{g\in G} (g-1)(e \otimes g^{-1}n_g) \in I_G(\mathbb{Z}[G] \otimes N) \,.$$

We conclude that $H_T^{-1}(G,M) = 0$. □

The exact sequence

$$0 \longrightarrow I_G \longrightarrow \mathbb{Z}[G] \longrightarrow \mathbb{Z} \longrightarrow 0 \tag{1.3}$$

is usually referred to as the *augmentation sequence*. Since $\mathbb{Z}$ is obviously a free $\mathbb{Z}$-module, it is split. Therefore, for any G-module M, the sequence obtained by tensoring the augmentation sequence with M

$$0 \longrightarrow I_G \otimes M \longrightarrow \mathbb{Z}[G] \otimes M \longrightarrow M \longrightarrow 0$$

is also exact and split.

Remark 2. The last exact sequence, together with the previous proposition, allows to extend some of the results that we have in classical cohomology to Tate cohomology by dimension shifting. For example, we can extend the natural maps restriction and corestriction, and we preserve the result that, for a subgroup H of G, the corresponding composite Cor $\circ$ Res is multiplication by $[G : H]$, so that Corollary 1.4.4 and Corollary 1.4.5 also hold with Tate cohomology. We can also generalize cup-products to Tate cohomology.

Let G^c be the commutator subgroup of G and let $G^{\mathrm{ab}} = G/G^c$.

Proposition 1.9.2. There is a canonical isomorphism

$$H_T^{-2}(G, \mathbb{Z}) \simeq G^{\mathrm{ab}} .$$

Proof. Consider the augmentation sequence (1.3). Since the middle group is induced, we get an isomorphism

$$\delta : H_T^{-2}(G, \mathbb{Z}) \to H_T^{-1}(G, I_G) = I_G/I_G^2 .$$

The group I_G is generated by the elements in $\mathbb{Z}[G]$ of the form $g - 1$, with $g \in G$, and I_G^2 is hence generated by the elements of the form $(g - 1)(g' - 1)$, with $g, g' \in G$.

We claim that the map

$$\begin{aligned} G &\to I_G/I_G^2 \\ g &\mapsto (g - 1) + I_G^2 \end{aligned}$$

induces an isomorphism

$$G/G^c \to I_G/I_G^2 .$$

First of all, let us check that it is in fact a homomorphism. To that end, observe that, for all $g, g' \in G$,

$$gg' - 1 = (g - 1) + (g' - 1) + (g - 1)(g' - 1) . \tag{1.4}$$

Since I_G is Abelian, this homomorphism factors through G^c, i.e. it induces a homomorphism

$$G/G^c \to I_G/I_G^2 ,$$

and, using again (1.4), the homomorphism $I_G \to G/G^c$ defined by $g - 1 \mapsto gG^c$ induces a homomorphism

$$I_G/I_G^2 \to G/G^c .$$

which is clearly an inverse of the previous one. □

Remark 3. In fact, it can be proved that there exists a canonical isomorphism $H_1(G,\mathbb{Z}) \simeq G^{\mathrm{ab}}$ for an arbitrary group G (not necessarily finite). The proof is quite similar to what we have done. In this case, working in homology, from the augmentation sequence we get an exact sequence

$$0 \longrightarrow H_1(G,\mathbb{Z}) \longrightarrow I_G/I_G^2 \longrightarrow \mathbb{Z}[G]/I_G \longrightarrow \mathbb{Z} \longrightarrow 0 \quad ,$$

and the fact that the map

$$\delta : H_1(G,\mathbb{Z}) \to H_0(G,I_G) = I_G/I_G^2$$

is an isomorphism can be deduced from the fact that the map

$$I_G/I_G^2 \to \mathbb{Z}[G]/I_G$$

is clearly the zero map.

Proposition 1.9.3. Let H be a subgroup of G. Then, the diagram

$$\begin{array}{ccc} H_T^{-2}(H,\mathbb{Z}) & \xrightarrow{\simeq} & H^{\mathrm{ab}} \\ \downarrow{\scriptstyle \mathrm{Cor}} & & \downarrow{\scriptstyle i} \\ H_T^{-2}(G,\mathbb{Z}) & \xrightarrow{\simeq} & G^{\mathrm{ab}} \end{array} \quad ,$$

where the horizontal arrows are given by the previous proposition and i is the map induced by the inclusion $H \hookrightarrow G$, commutes.

Proof. We have the diagram

$$\begin{array}{ccccc} H^{\mathrm{ab}} & \xrightarrow{\sigma \mapsto \sigma - 1} & H_T^{-1}(H,I_H) & \xleftarrow[\delta]{} & H_T^{-2}(H,\mathbb{Z}) \\ & & \downarrow & & \downarrow{\scriptstyle =} \\ & & H_T^{-1}(H,I_G) & \xleftarrow[\delta]{} & H_T^{-2}(H,\mathbb{Z}) \\ & & \downarrow{\scriptstyle \mathrm{Cor}} & & \downarrow{\scriptstyle \mathrm{Cor}} \\ G^{\mathrm{ab}} & \xrightarrow{\sigma \mapsto \sigma - 1} & H_T^{-1}(G,I_G) & \xleftarrow[\delta]{} & H_T^{-2}(G,\mathbb{Z}) \end{array} \quad ,$$

where the δ maps are the connecting maps coming from the corresponding augmentation sequences. Observe that the homomorphisms in the first and third row are precisely those defining the isomorphisms $H^{\mathrm{ab}} \simeq H_T^{-2}(H,\mathbb{Z})$ and $G^{\mathrm{ab}} \simeq H_T^{-2}(G,\mathbb{Z})$, respectively.

The vertical arrow $H_T^{-1}(H,I_H) \to H_T^{-1}(H,I_G)$ is the map induced by the inclusion $I_H \hookrightarrow I_G$. The upper square commutes since we have the commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & I_H & \longrightarrow & \mathbb{Z}[H] & \longrightarrow & \mathbb{Z} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle i} & & \downarrow{\scriptstyle i} & & \downarrow{\scriptstyle =} & & \\ 0 & \longrightarrow & I_G & \longrightarrow & \mathbb{Z}[G] & \longrightarrow & \mathbb{Z} & \longrightarrow & 0 \end{array} \quad .$$

The bottom square commutes since corestriction is compatible with the connecting maps.

The map $H_0(H, I_H) \to H_0(H, I_G)$ induced by the inclusion $I_H \hookrightarrow I_G$ is just the natural map $I_H/I_H^2 \to I_G/I_H I_G$. Therefore, the vertical arrow $H_T^{-1}(H, I_H) \to H_T^{-1}(H, I_G)$ is the natural map

$$I_H/I_H^2 = H_T^{-1}(H, I_H) \to H_T^{-1}(H, I_G) \subseteq I_G/I_H I_G\,.$$

We use dimension shifting to find a description of the vertical arrow

$$\mathrm{Cor} : H_T^{-1}(H, I_G) \to H_T^{-1}(G, I_G)\,.$$

From the exact sequence of G-modules

$$0 \longrightarrow I_G \otimes I_G \longrightarrow \mathbb{Z}[G] \otimes I_G \longrightarrow I_G \longrightarrow 0$$

we get the commutative diagram

$$\begin{array}{ccc} H_T^{-1}(H, I_G) & \xrightarrow{\delta} & H_T^0(H, I_G \otimes I_G) \\ \downarrow{\scriptstyle \mathrm{Cor}} & & \downarrow{\scriptstyle \mathrm{Cor}} \\ H_T^{-1}(G, I_G) & \xrightarrow{\delta} & H_T^0(G, I_G \otimes I_G) \end{array}\,.$$

For any element $\bar{x} \in H_T^{-1}(H, I_G)$ being the class of $x \in I_G$, its image under the first horizontal arrow can be obtained as the class of $\mathrm{Nm}_H(1 \otimes x)$ in $H_T^0(H, I_G \otimes I_G)$. Going now downwards, and using the commutative diagram (1.2), we obtain the class of

$$\mathrm{Nm}_{G/H}(\mathrm{Nm}_H(1 \otimes x)) = \mathrm{Nm}_G(1 \otimes x),$$

and a preimage of this element in $H^{-1}(G, I_G)$ is clearly the class of x in $H_T^{-1}(G, I_G)$. Since the bottom arrow is an isomorphism, this shows that the corestriction map $H_T^{-1}(H, I_G) \to H_T^{-1}(G, I_G)$ is just given by the natural map

$$I_G/I_H I_G \to I_G/I_G^2\,.$$

Putting all together, we obtain the desired result. □

Lemma 1.9.4. Let H be a subgroup of G of finite index (here G is not necessarily finite) and let $S = \{s_i\}_{1 \leqslant i \leqslant n}$ be a system of representatives for the right cosets of H in G. Given $g \in G$, let $\varphi(g)$ be the element in S lying in the same right coset. Then, the map

$$g \mapsto \prod_{i=1}^{n} s_i g \varphi(s_i g)^{-1} \pmod{H'}$$

defines a homomorphism $G \to H/H^c$ and hence induces a homomorphism $G/G^c \to H/H^c$.

Proof. Observe that, for any $g \in G$, if we write

$$s_i g = h_i s_i'$$

for all $i = 1, \ldots, n$, with $s_i' \in S$ and $h_i \in H$, then

$$s_i g \varphi(s_i g)^{-1} = h_i\,.$$

Also observe that all the s_i' are distinct, for if $s_i' = s_j'$ then $h_i^{-1} s_i = h_j^{-1} s_j$ so that s_i and s_j would lie in the same right coset. The result is now completely straightforward taking into account these observations. □

Definition 1.9.5. The map $G/G^c \to H/H^c$ from the previous lemma is called the *transfer map* or the *Verlagerung* map from G to H and is denoted by

$$\mathrm{Ver} : G/G^c \to H/H^c\,.$$

Proposition 1.9.6. Let H be a subgroup of G. Then, the diagram

$$\begin{array}{ccc} H_T^{-2}(G,\mathbb{Z}) & \xrightarrow{\simeq} & G^{\mathrm{ab}} \\ \downarrow{\scriptstyle \mathrm{Res}} & & \downarrow{\scriptstyle \mathrm{Ver}} \\ H_T^{-2}(H,\mathbb{Z}) & \xrightarrow{\simeq} & H^{\mathrm{ab}} \end{array},$$

where the horizontal arrows are the isomorphisms from Proposition 1.9.2, commutes.

Proof. Similarly to what we did in the proof of Proposition 1.9.3, we get the commutative diagram

$$\begin{array}{ccccc} H^{\mathrm{ab}} & \xrightarrow{\sigma\mapsto\sigma-1} & H_T^{-1}(H,I_H) & \xleftarrow[\delta]{} & H_T^{-2}(H,\mathbb{Z}) \\ & & \downarrow & & \downarrow{\scriptstyle =} \\ & & H_T^{-1}(H,I_G) & \xleftarrow[\delta]{} & H_T^{-2}(H,\mathbb{Z}) \\ & & \uparrow{\scriptstyle \mathrm{Res}} & & \uparrow{\scriptstyle \mathrm{Res}} \\ G^{\mathrm{ab}} & \xrightarrow{\sigma\mapsto\sigma-1} & H_T^{-1}(G,I_G) & \xleftarrow[\delta]{} & H_T^{-2}(G,\mathbb{Z}) \end{array},$$

where the composite of the arrows in the first and in the third row provide the isomorphisms $H^{\mathrm{ab}} \simeq H_T^{-2}(H,\mathbb{Z})$ and $G^{\mathrm{ab}} \simeq H_T^{-2}(G,\mathbb{Z})$ from Proposition 1.9.2. We already know that the connecting maps δ in the first and third rows are isomorphisms, and the connecting map $H_T^{-2}(H,\mathbb{Z}) \to H_T^{-1}(H,I_G)$ is injective because $\mathbb{Z}[G]$ is a free $\mathbb{Z}[H]$-module. Therefore, the vertical arrow $H_T^{-1}(H,I_H) \to H_T^{-1}(H,I_G)$ is also an injective homomorphism.

Hence, we need only prove that, for any $g \in G$, and following the diagram, the elements $gG^c \in G/G^c$ and $\mathrm{Ver}(gG^c) \in H/H^c$ have the same image in $H_T^{-1}(H,I_G)$. Let us first determine explicitly the map $\mathrm{Res} : H_T^{-1}(G,I_G) \to H_T^{-1}(H,I_G)$. To that end, we use dimension shifting in a similar fashion to what we did in the proof of Proposition 1.9.3. We have a commutative diagram

$$\begin{array}{ccc} H_T^{-1}(G,I_G) & \xrightarrow{\delta} & H_T^{0}(G,I_G\otimes I_G) \\ \downarrow{\scriptstyle \mathrm{Res}} & & \downarrow{\scriptstyle \mathrm{Res}} \\ H_T^{-1}(H,I_G) & \xrightarrow{\delta} & H_T^{0}(H,I_G\otimes I_G) \end{array}.$$

Take any element $\overline{x} \in H_T^{-1}(G,I_G)$ being the class of $x \in I_G$. Going to the right in the previous diagram we obtain the class of $\mathrm{Nm}_G(1\otimes x)$ in $H_T^0(G,I_G\otimes I_G)$, and, going now downwards, we obtain the class of this same element in $H_T^0(H,I_G\otimes I_G)$. A preimage of this element in $H_T^{-1}(H,I_G)$ is the class of $\mathrm{Nm}_{H\backslash G}x$, where the definition of $\mathrm{Nm}_{H\backslash G}$ is analogous to that of $\mathrm{Nm}_{G/H}$ using right coset representatives. To see it, observe that, given right coset representives $s_1,\dots,s_n$ of H in G,

$$\begin{aligned} \mathrm{Nm}_H(1\otimes \mathrm{Nm}_{H\backslash G}x) = \sum_{h\in H}\sum_{i=1}^{n} h\otimes hg_ix \equiv \sum_{h\in H}\sum_{i=1}^{n} hg_i\otimes hg_ix = \\ = \mathrm{Nm}_G(1\otimes x) \pmod{\mathrm{Nm}_H(I_G\otimes I_G)}\,. \end{aligned}$$

Since the connecting maps in the previous diagram are isomorphisms, this shows that the map $\mathrm{Res} : H_T^{-1}(G, I_G) \to H_T^{-1}(H, I_G)$ is induced by $\mathrm{Nm}_{H\backslash G}$.

Now, take any gG^c. Its image in $H_T^{-1}(H, I_G)$ in the commutative diagram 1.9 is the class of the element $\mathrm{Nm}_{H\backslash G}(g-1)$. Let S be a system of representatives of the right cosets of H in G, and let $sg = h_s s'$ with $s' \in S$ and $h_s \in H$ for all $s \in S$. Then $\mathrm{Ver}(gG^c)$ is the class of $\prod_{s\in S} h_s$ in H^{ab}. Its image in $H_T^{-1}(H, I_G)$ is $\sum_{s\in S}(h_s - 1)$, and we have

$$\mathrm{Nm}_{H\backslash G}(g-1) = \sum_{s\in S} s(g-1) = \sum_{s\in S} h_s s' - \sum_{s\in S} s = \sum_{s\in S}(h_s - 1)s' \equiv \sum_{s\in S}(h_s - 1) \pmod{I_H I_G}.$$

□

Lemma 1.9.7. Let $n = |G|$. Then, we have the following results:

1. $H_T^r(G, \mathbb{Q}) = 0$ for all $r \in \mathbb{Z}$.
2. $H_T^0(G, \mathbb{Z}) = \mathbb{Z}/n\mathbb{Z}$ and $H^1(G, \mathbb{Z}) = 0$.

(As usually, we are considering $\mathbb{Z}$ and $\mathbb{Q}$ as G-modules with trivial action.)

Proof. For the first statement, observe that, for every non-zero integer m, multiplication by m defines an isomorphism $\mathbb{Q} \to \mathbb{Q}$, and, therefore, it provides isomorphisms $H_T^r(G, \mathbb{Q}) \to H_T^r(G, \mathbb{Q})$ which are also multiplication by m. Since, for all $r \in \mathbb{Z}$, we have $nH_T^r(G, \mathbb{Q}) = 0$ (see Corollary 1.4.4), we deduce that $H_T^r(G, \mathbb{Q}) = 0$ for all $r \in \mathbb{Z}$.

For the second statement, we have, by definition,

$$H_T^0(G, \mathbb{Z}) = \mathbb{Z}^G/\mathrm{Nm}_G\mathbb{Z}.$$

Since G acts trivially on $\mathbb{Z}$, we have that $\mathbb{Z}^G = \mathbb{Z}$ and, moreover, that the norm map is simply multiplication by n, whereby we obtain

$$H_T^0(G, \mathbb{Z}) = \mathbb{Z}/n\mathbb{Z}.$$

On the other hand, also because the action of G on $\mathbb{Z}$ is trivial, we know that $H^1(G, \mathbb{Z}) \simeq \mathrm{Hom}(G, \mathbb{Z})$. But, since G is finite, any homomorphism $G \to \mathbb{Z}$ must map every element in G to zero, so that we deduce that $H^1(G, \mathbb{Z}) = 0$. □

Remark 4. Since $H_T^r(G, \mathbb{Q}) = 0$ for all $r \in \mathbb{Z}$, the exact sequence

$$0 \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Q} \longrightarrow \mathbb{Q}/\mathbb{Z} \longrightarrow 0$$

provides an isomorphism

$$\mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z}) \simeq H^1(G, \mathbb{Q}/\mathbb{Z}) \xrightarrow{\delta} H^2(G, \mathbb{Z}).$$

Proposition 1.9.8. Assume that G is cyclic, and let M be a G-module. Then, the choice of a generator of G provides isomorphisms

$$H_T^r(G, M) \xrightarrow{\simeq} H_T^{r+2}(G, M)$$

for all $r \in \mathbb{Z}$.

Proof. Let σ be a generator of G. Then, the sequence

$$0 \longrightarrow \mathbb{Z} \xrightarrow{m \mapsto \sum_{g \in G} mg} \mathbb{Z}[G] \xrightarrow{\sigma - 1} I_G \longrightarrow 0$$

is exact (observe that $\sigma^j - 1 = (\sigma - 1)(1 + \sigma + \cdots + \sigma^{j-1})$). Since all the groups involved are free $\mathbb{Z}$-modules, tensoring with M we obtain an exact sequence

$$0 \longrightarrow M \longrightarrow \mathbb{Z}[G] \otimes M \longrightarrow I_G \otimes M \longrightarrow 0$$

which, since the middle group is induced, provides an isomorphism

$$H_T^{r+1}(G, I_G \otimes M) \to H_T^{r+2}(G, M)\,.$$

We also have the exact sequence obtained by tensoring the augmentation sequence with M, i.e.

$$0 \longrightarrow I_G \otimes M \longrightarrow \mathbb{Z}[G] \otimes M \longrightarrow M \longrightarrow 0\,,$$

which provides an isomorphism

$$H_T^{r}(G, M) \to H_T^{r+1}(G, I_G \otimes M)\,.$$

Combining the isomorphisms which we have obtained, we obtain an isomorphism

$$H_T^{r}(G, M) \to H_T^{r+2}(G, M)\,.$$

□

Remark 5. The isomorphisms in the proposition obtained from a certain generator σ of G are compatible with the maps in the long exact sequence of Tate cohomology groups obtained from a short exact sequence of G-modules (this follows easily from the explicit description of these maps using chains and cochains). In fact, if $\chi \in \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z}) \simeq H^1(G, \mathbb{Z})$ is the character mapping the chosen generator σ to $1/|G| + \mathbb{Z} \in \mathbb{Q}/\mathbb{Z}$ and $\delta\chi$ is its image in $H^2(G, \mathbb{Z})$ under the connecting isomorphism $H^1(G, \mathbb{Q}/\mathbb{Z}) \to H^2(G, \mathbb{Z})$, then the isomorphisms $H^r(G, M) \to H^{r+2}(G, M)$ obtained in the proposition are given by $x \mapsto x \cup \delta\chi$ (a straightforward but lengthy calculation allows to prove this for $r > 0$ using cochains and then we generalize the result for all r by dimension shifting).

Definition 1.9.9. Assume that G is cyclic and let M be a G-module. Then, if the cohomology groups of $H_T^r(G, M)$ are finite, the *Herbrand quotient of* M is

$$h(G, M) = \frac{|H_T^0(G, M)|}{|H_T^1(G, M)|}\,.$$

Remark 6. By the previous proposition, all even Tate cohomology groups are isomorphic, and all odd Tate cohomology groups are isomorphic, so that the Herbrand quotient can actually be calculated from any pair of an even and an odd Tate cohomology group.

Proposition 1.9.10. Assume that G is cyclic and let

$$0 \longrightarrow M \longrightarrow M' \longrightarrow M'' \longrightarrow 0$$

be an exact sequence of G-modules. Then, whenever any two of the Herbrand quotients $h(G,M)$, $h(G,M')$ and $h(G,M'')$ are defined, so is the third and it holds

$$h(G,M') = h(G,M)\cdot h(G,M'')\,.$$

Proof. We can truncate the cohomology sequence corresponding to the given short exact sequence as

$$\begin{aligned} 0 \longrightarrow A \longrightarrow H^0_T(G,M) \longrightarrow H^0_T(G,M') \longrightarrow H^0_T(G,M'') \longrightarrow \\ \longrightarrow H^1_T(G,M) \longrightarrow H^1_T(G,M') \longrightarrow H^1_T(G,M'') \longrightarrow B \longrightarrow 0 \end{aligned}$$

where

$$\begin{aligned} A &= \ker(H^0_T(G,M) \to H^0_T(G,M')) \\ B &= \operatorname{coker}(H^1_T(G,M') \to H^1_T(G,M'')) \simeq \ker(H^2_T(G,M) \to H^2_T(G,M'))\,. \end{aligned}$$

Because of Proposition 1.9.8, and taking into account the remark following it, we have $A \simeq B$.

Now, it is straightforward that whenever the Tate cohomology groups of two of the modules in the given short exact sequence are finite, so are those of the third, and in this case the identity

$$h(G,M') = h(G,M)\cdot h(G,M'')$$

follows from the well-known result stating that the alternated product of the orders of the groups in an exact sequence is 1. □

Proposition 1.9.11. Assume that G is cyclic. Then, for any finite G-module M,

$$h(G,M) = 1\,.$$

Proof. Let σ be a generator of G. Then, we have an exact sequence

$$0 \longrightarrow M^G \longrightarrow M \xrightarrow{\sigma - 1} M \longrightarrow M_G \longrightarrow 0$$

from which we deduce that M^G and M_G have the same order. Hence, from the exact sequence

$$0 \longrightarrow H^{-1}_T(G,M) \longrightarrow M_G \xrightarrow{\mathrm{Nm}_G} M^G \longrightarrow H^0_T(G,M) \longrightarrow 0$$

we obtain that $H^{-1}_T(G,M)$ and $H^0_T(G,M)$ have the same order, and the desired result follows. □

Corollary 1.9.12. Assume that G is cyclic and let $\alpha : M \to N$ be a homomorphism of G-modules with finite kernel and cokernel. Then, whenever any of the Herbrand quotients $h(G,M)$ and $h(G,N)$ is defined, so is the other and $h(G,M) = h(G,N)$.

Proof. Consider the exact sequences of G-modules

$$0 \longrightarrow \ker\alpha \longrightarrow M \longrightarrow \alpha(M) \longrightarrow 0$$

and

$$0 \longrightarrow \alpha(M) \longrightarrow N \longrightarrow \mathrm{coker}\alpha \longrightarrow 0$$

.

Since $\ker\alpha$ and $\mathrm{coker}\alpha$ are finite, their Herbrand quotients are always defined and equal 1. Therefore, if $h(G,M)$ is defined, from the first exact sequence we deduce that $h(G,\alpha(M))$ is defined and equals $h(G,M)$, and then from the second exact sequence we deduce that $h(G,N)$ is defined and equals $h(G,M)$. In the same way, if $h(G,N)$ is defined, from the second exact sequence $h(G,\alpha(M))$ is defined and equals $h(G,N)$, and then from the first exact sequence $h(G,M)$ is defined and equals $h(G,N)$. □

Proposition 1.9.13. Let M be a G-module such that $H^1(H,M)=0$ and $H^2(H,M)=0$ for all subgroup H of G. Then,

$$H_T^r(G,M)=0 \quad \text{for all } r\in\mathbb{Z}.$$

Proof. If G is cyclic, the result follows from Proposition 1.9.8.

Now, we will prove the result in the case that G is solvable by induction on the order of G. So assume that G is a solvable group, assume that M is a G-module for which the hypothesis of the proposition holds, and suppose that the result has already been proved for all solvable groups K of order less than G and all K-modules. Since we are assuming that G is solvable, there is a proper normal subgroup H of G such that G/H is cyclic. Then, if the hypothesis of the proposition holds for G and M it clearly holds for H and M, so that, applying the induction hypothesis, we have $H_T^r(H,M)=0$ for all $r\in\mathbb{Z}$. Then, using Proposition 1.4.6, we have exact sequences

$$0 \longrightarrow H_T^r(G/H,M^H) \xrightarrow{\text{Inf}} H_T^r(G,M) \xrightarrow{\text{Res}} H_T^r(H,M)$$

for all $r>0$. Since $H_T^1(G,M)=0$ and $H_T^2(G,M)=0$, from these exact sequences we deduce that $H_T^1(G/H,M^H)=0$ and $H_T^2(G/H,M^H)=0$, and, therefore, since G/H is cyclic, we deduce that $H_T^r(G/H,M^H)=0$ for all $r\in\mathbb{Z}$. Hence, using again the Inflation-Restriction sequences, we deduce that $H_T^r(G,M)=0$ for all $r>0$.

Now, since $H_T^0(G/H,M^H)=0$, for any $x\in M^G$ there exists some $y\in M^H$ such that $x=\mathrm{Nm}_{G/H}(y)$, and, since $H_T^0(H,M)=0$, there exists some $z\in M$ such that $y=\mathrm{Nm}_H(z)$, so that

$$x=\mathrm{Nm}_{G/H}(\mathrm{Nm}_H(z))=\mathrm{Nm}_G(z)\,,$$

which shows that $H_T^0(G,M)=0$.

Consider the exact sequence

$$0 \longrightarrow I_G\otimes M \longrightarrow \mathbb{Z}[G]\otimes M \longrightarrow M \longrightarrow 0$$

obtained by tensoring the augmentation sequence with M. Since the middle group is induced, from this sequence we get isomorphisms

$$H_T^r(H,M)\simeq H_T^{r+1}(H,I_G\otimes M)$$

for all subgroup H of G. From these isomorphisms, we see that $H_T^1(H,I_G\otimes M)=0$ and $H_T^2(H,I_G\otimes M)=0$ for all subgroup H of G, i.e. the hypothesis of the proposition is also satisfied for G and $I_G\otimes M$. Consequently, we know that $H_T^0(G,I_G\otimes M)=0$, which implies that $H_T^{-1}(G,M)=0$. But now, we know that for any G-module N satisfying the hypothesis of the proposition, we have $H_T^{-1}(G,N)=0$, so that $H_T^{-1}(G,I_G\otimes M)=0$ and consequently $H_T^{-2}(G,M)=0$. Continuing in this way, we see that $H_T^r(G,M)=0$ for all $r\in\mathbb{Z}$.

Finally, assume now that G is any finite group and M a G-module. For any prime p and for any p-Sylow subgroup G_p of G, the hypothesis of the theorem holds with G_p and M, so that, since G_p is solvable, we know that $H^r_T(G_p, M) = 0$ for all $r \in G$. Since, for all $r \in \mathbb{Z}$, the map $\mathrm{Res} : H^r_T(G, M) \to H^r_T(G_p, M)$ is injective on the p-primary component of $H^r_T(G, M)$ (see Corollary 1.4.5), this p-primary component must be zero. Since this is true for all prime p, we deduce that, for all $r \in \mathbb{Z}$, we have $H^r_T(G, M) = 0$. □

Theorem 1.9.14. (Tate's theorem) Let M be a G-module such that, for all subgroup H of G, it holds that $H^1(H, M) = 0$ and $H^2(H, M)$ is a cyclic group of order $|H|$. Then, for every generator γ of the cyclic group $H^2(G, M)$, cup-product with γ defines an isomorphism

$$H^r_T(G, \mathbb{Z}) \xrightarrow{\cup\gamma} H^{r+2}_T(G, M)\,.$$

Proof. For every subgroup H of G, since $(\mathrm{Cor} \circ \mathrm{Res})(\gamma) = [G : H]\gamma$, we see that $(\mathrm{Cor} \circ \mathrm{Res})(\gamma)$ has order $|H|$. Therefore $\mathrm{Res}(\gamma)$ has order a multiple of $|H|$ in $H^2(H, M)$, so that, since this group is cyclic of order $|H|$, we see that $\mathrm{Res}(\gamma)$ is a generator of $H^2(H, M)$.

Let $\varphi : G^2 \to \mathbb{Z}$ be a cochain representing γ. Define the group $M(\varphi)$ as the direct sum of M and the free Abelian group having as basis $\{x_\sigma\}_{\sigma \in G\setminus\{1\}}$, and define an action of G on $M(\varphi)$ which acts as the action of G on M on the elements of M and such that

$$\sigma x_\tau = x_{\sigma\tau} - x_\sigma + \varphi(\sigma, \tau) \tag{1.5}$$

for all $\sigma, \tau \in G$, setting $x_1 = \varphi(1, 1)$. To check that this actually provides an action, observe that, since φ is a cocycle, we have the identity

$$g_1\varphi(g_2, g_3) - \varphi(g_1g_2, g_3) + \varphi(g_1, g_2g_3) - \varphi(g_1, g_2) = 0 \quad \text{for all } g_1, g_2, g_3 \in G\,.$$

Substituting $g_1 = \sigma$ and $g_2 = g_3 = 1$, we get $\sigma\varphi(1, 1) = \varphi(\sigma, 1)$, which shows that, for $\tau = 1$, the action given by equation (1.5) coincides with the action on M. Substituting $g_2 = g_3 = 1$ and $g_3 = \tau$ shows that $1x_\tau = x_\tau$. Finally,

$$\begin{aligned}\rho(\sigma x_\tau) &= \rho(x_{\sigma\tau} - x_\sigma + \varphi(\sigma, \tau)) = x_{\rho\sigma\tau} - x_\rho + \varphi(\rho, \sigma\tau) - (x_{\rho\sigma} - x_\rho + \varphi(\rho, \sigma)) + \rho\varphi(\sigma, \tau)) = \\ &= x_{\rho\sigma\tau} - x_{\rho\sigma} + \varphi(\rho\sigma, \tau) = (\rho\sigma)(x_\tau)\,.\end{aligned}$$

Now, let $\alpha : G \to M(\varphi)$ be the cochain mapping each $\sigma \in G$ to x_σ. Then,

$$\mathrm{d}\alpha(\sigma, \tau) = \sigma x_\tau - x_{\sigma\tau} + x_\sigma = \varphi(\sigma, \tau)\,,$$

which shows that γ maps to zero in $H^2(G, M(\varphi))$.

From the augmentation sequence (1.3) and Lemma 1.9.7 we get isomorphisms

$$\begin{aligned}H^1(H, I_G) &\simeq H^0_T(H, \mathbb{Z}) \simeq \mathbb{Z}/|H|\mathbb{Z} \\ H^2(H, I_G) &\simeq H^1(H, \mathbb{Z}) = 0\,.\end{aligned}$$

Let $\beta : M(\varphi) \to I_G$ be the homomorphism satisfying $\beta(m) = 0$ for all $m \in M$ and $\beta(x_\sigma) = \sigma - 1$ for all $\sigma \in G$. Then, the sequence

$$0 \longrightarrow M \longrightarrow M(\varphi) \xrightarrow{\beta} I_G \longrightarrow 0$$

is exact. This short exact sequence provides, for each subgroup H of G, an exact sequence

$$0 \longrightarrow H^1(H, M(\varphi)) \longrightarrow H^1(H, I_G) \longrightarrow H^2(H, M) \longrightarrow H^2(H, M(\varphi)) \longrightarrow 0$$

(we have taken into account that $H^1(H, M) = 0$ and $H^2(H, I_G) = 0$). The map $H^2(H, M) \to H^2(H, M(\varphi))$ is zero because $H^2(H, M)$ is generated by $\mathrm{Res}(\gamma)$, which maps to the restriction of the image of γ in $H^2(G, M(\varphi))$, which is zero. Hence, the middle arrow is surjective, and so is an isomorphism, because the groups $H^1(H, I_G)$ and $H^2(H, M)$ have both order $|H|$. Then, we have that $H^1(H, M(\varphi)) = 0$ and $H^2(H, M(\varphi)) = 0$ for all subgroup H of G, which, because of the previous proposition, implies that $H^r_T(G, M(\varphi)) = 0$ for all $r \in \mathbb{Z}$.

The composite of the isomorphism

$$\delta : H^r_T(G, \mathbb{Z}) \xrightarrow{\simeq} H^{r+1}_T(G, I_G)$$

obtained from the augmentation sequence and the isomorphism

$$\delta' : H^{r+1}_T(G, I_G) \xrightarrow{\simeq} H^{r+2}_T(G, M)$$

obtained from the exact sequence

$$0 \longrightarrow M \longrightarrow M(\varphi) \xrightarrow{\beta} I_G \longrightarrow 0$$

provides an isomorphism

$$H^r_T(G, \mathbb{Z}) \xrightarrow{\simeq} H^{r+2}_T(G, M)\,.$$

Let us check that this isomorphism is cup-product with γ. To that end, we will use the properties of cup-products involving exact sequences taking into account that tensoring an exact sequence with $\mathbb{Z}$ leaves it unchanged. For any $x \in H^r(G, \mathbb{Z})$, we have

$$\delta'\delta x = \delta'\delta(x) \cup 1 = \delta'(\delta x \cup 1) = \delta'\delta(x \cup 1) = (-1)^r \delta'(x \cup \delta 1) = x \cup \delta'\delta 1\,,$$

where 1 denotes the class of $1 \in \mathbb{Z}$ in $H^0_T(G, \mathbb{Z})$. The element $\delta 1 \in H^1(G, I_G)$ is represented by the 1-cochain $f : G \to I_G$ defined by

$$f(\sigma) = \sigma - 1 \quad \text{for all } \sigma \in G\,.$$

To obtain $\delta'\delta 1$, observe that for any $\sigma \in G$, a preimage of $\sigma - 1$ by the homomorphism β is given by x_σ, so that $\delta'\delta 1$ is represented by the 2-cochain $g : G^2 \to M$ defined by

$$g(\sigma, \tau) = \sigma x_\tau - x_{\sigma\tau} + x_\sigma = \varphi(\sigma, \tau) \quad \text{for all } \sigma, \tau \in G\,.$$

Since $g = \varphi$, we see that $\delta'\delta 1 = \gamma$. □

Chapter 2

Valuations and local fields

In this chapter we present the basics of the theory of valuations and local fields.

2.1 Valuations

References: [Neu99], [Mil17a], [Mil13]

Throughout this section, K will always denote a field.

Definition 2.1.1. A *(multiplicative) valuation* on K is a map $|\cdot| : K \to \mathbb{R}$ satisfying:

1. $|x| \geqslant 0$ for all $x \in K$ and $|x| = 0 \Leftrightarrow x = 0$.
2. $|xy| = |x||y|$.
3. $|x + y| \leqslant |x| + |y|$.

Remark 7. We will refer to the valuation such that $|x| = 1$ for all $x \in K^\times$ as the *trivial valuation*, and we will often exclude it.

Definition 2.1.2. A *valued field* is a field K provided with a valuation $|\cdot|$.

Definition 2.1.3. A valuation $|\cdot|$ is *arquimedian* if the set $\{|n| : n \in \mathbb{N}\}$ is unbounded. Otherwise, it is *non-archimedian*.

For example, for $K = \mathbb{Q}$, the classical absolute value is an archimedian valuation, whereas, for any prime p, the corresponding p-adic valuation, defined as $|x|_p = p^{-\mathrm{ord}_p(x)}$, is non-archimedian.

Lemma 2.1.4. A valuation $|\cdot|$ is non-archimedian if an only if it satisfies the condition

$$|x + y| \leqslant \max\{|x|, |y|\},$$

which is known as the *strong triangle inequality*.

Proof. If a valuation $|\cdot|$ satisfies the strong triangle inequality, then it is clear, by induction, that $|n| \leqslant |1|$, so that the set $\{|n| : n \in \mathbb{N}\}$ is clearly bounded.

Now, assume that the set $\{|n| : n \in \mathbb{N}\}$ is bounded. Take $M > 0$ such that $|n| \leqslant M$ for all integer n. Then, for all $n > 0$,

$$|x + y|^n = \left| \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k} \right| \leqslant M(n+1) \max\{|x|^n, |y|^n\},$$

and, therefore, for all $n > 0$,

$$|x+y| \leqslant M^{1/n}(n+1)^{1/n} \max\{|x|, |y|\}\,.$$

Letting n tend to infinity, we get the strong triangle inequality. □

Remark 8. In fact, it is easy to prove that $|x+y| = \max\{|x|, |y|\}$ whenever $|x| \neq |y|$.

Observe that any multiplicative valuation induces a distance on K (given by $d(x,y) = |x-y|$) and, consequently, a topology.

Definition 2.1.5. Two valuations $|\cdot|_1$, $|\cdot|_2$ are *equivalent* if they define the same topology on the field K.

Lemma 2.1.6. Let $|\cdot|_1$, $|\cdot|_2$ be valuations on K and assume that $|\cdot|_1$ is non-trivial. Then, the following conditions are equivalent:

1. $|\cdot|_1$ and $|\cdot|_2$ are equivalent valuations.
2. $|x|_1 < 1 \Rightarrow |x|_2 < 1$.
3. There is a constant $c > 0$ such that $|\cdot|_1 = |\cdot|_2^c$.

Proof. We begin by proving $1 \Rightarrow 2$. Let $|\cdot|_1$ and $|\cdot|_2$ be equivalent valuations on K, so that they define the same topology. Assume that, for some $x \in K$, $|\cdot|_1 < 1$. Therefore, the sequence $(a_n)_n$, with $a_n = x^n$, has limit zero with this topology, as $\lim_n |x|_1^n = 0$. But, since both valuations induce the same topology, this necessarily implies that $\lim_n |x|_2^n = 0$, and therefore $|x|_2 < 1$.

Now, let us prove $2 \Rightarrow 3$. Fix an element $x \in K$ such that $|x|_1 > 1$. Take any element $y \in K$. There exist $\alpha, \beta \in \mathbb{R}$ such that $|y|_1 = |x|_1^\alpha$ and $|y|_2 = |x|_2^\beta$. Take a sequence of rational numbers m_i/n_i, where m_i and n_i are integers and $n_i \neq 0$ for all i, which tends to α from below. Then,

$$\left|\frac{x^{m_i}}{y^{n_i}}\right|_1 = \left(\frac{|x|_1^{m_i/n_i}}{|y|_1}\right)^{n_i} < 1\,,$$

so that,

$$\left(\frac{|x|_2^{m_i/n_i}}{|y|_2}\right)^{n_i} = \left|\frac{x^{m_i}}{y^{n_i}}\right|_2 < 1\,.$$

Since m_i/n_i tends to α, this implies that $\beta \geqslant \alpha$. Analogously we prove that $\beta \leqslant \alpha$, so that $\beta = \alpha$. Take $c \in \mathbb{R}$ such that $|x|_2 = |x|_1^c$. The constant c must be positive, as

$$|x|_1 > 1 \Rightarrow |x|_2 > 1$$

by simply taking inverses in the given condition. Then we find

$$|y|_2 = |x|_2^\alpha = |x|_1^{c\alpha} = |y|_1^c\,.$$

Finally, the implication $3 \Rightarrow 1$ is trivial. □

For $K = \mathbb{Q}$ we have the valuation corresponding to the classical absolute value, which we will denote by $|\cdot|_\infty$, and the p-adic valuations corresponding to each prime. It is easy to check that all these valuations are inequivalent. The following theorem tells us that, up to equivalence, these are all the non-trivial valuations of $\mathbb{Q}$.

Theorem 2.1.7. (Ostrowski) Let $|\cdot|$ be a non-trivial valuation on $\mathbb{Q}$. Then, if it is archimedian, it is equivalent to $|\cdot|_\infty$, and, otherwise, it is equivalent to $|\cdot|_p$ for some prime p.

Proof. First consider that $|\cdot|$ is archimedian. Take any pair of integers $m, n > 1$. Let $M_n = \max\{1, |n|\}$. The integer m can be written in the form

$$m = a_0 + a_1 n + \dots a_r n^r$$

for some integers a_i with $0 \leqslant a_i < n$ and some $r \leqslant 0$. We can obviously assume $a_r > 0$, so that $n^r \leqslant m$ and therefore

$$r \leqslant \frac{\log m}{\log n}\,.$$

Also, observe that $|a_i| \leqslant a_i|1| = a_i \leqslant n$. Hence, we get

$$|m| \leqslant n(r+1)M_n^r \leqslant n\left(\frac{\log m}{\log n} + 1\right) M_n^{\log m/\log n}\,.$$

The same argument with m^k, for all integer $k > 0$, shows that

$$|m|^k \leqslant n\left(k\frac{\log m}{\log n} + 1\right) M_n^{k\log m/\log n}$$

which, taking k-th roots and letting k tend to infinity, gives

$$|m| \leqslant M_n^{\log m/\log n}\,.$$

If $M_n = 1$, we get that $|m| \leqslant 1$ for all integer m, contradicting the assumption that the valuation is archimedian. Therefore, $|n| > 1$ for all $n > 1$, so that

$$|m| \leqslant |n|^{\log m/\log n}\,,$$

and, in the same way,

$$|n| \leqslant |m|^{\log n/\log m}\,,$$

so that

$$|m|^{1/\log m} = |n|^{1/\log n}$$

for all integers $m, n > 1$. Therefore, defining

$$c = \frac{\log|m|}{\log m}$$

for any integer $m > 1$, we get that

$$|n| = |n|_\infty^c$$

for all positive integer $n > 1$. But this condition and the multiplicativity of the valuation clearly implies

$$|x| = |x|_\infty^c$$

for all $x \in \mathbb{Q}$.

Now, suppose that $|\cdot|$ is non-archimedian. Then, $|n| \leqslant 1$ for all integer n. Since the valuation is non-trivial, and, by multiplicativity, it is determined by its value on the primes, there must exist some prime p such that $|p| < 1$. If there were two different such primes, a simple application of Bézout identity and the strong triangle inequality would yield $|1| < 1$, which is not possible.

Therefore, there exists some prime p such that $|p| < 1$ and $|q| = 1$ at any other prime. Hence, for any $x = up^r \in \mathbb{Q}$, with $\mathrm{ord}_p(u) = 0$,

$$|x| = |p|^r = p^{-rc} = |x|_p^c \,,$$

where $c = \log|p|/\log p$. □

Definition 2.1.8. An *exponential valuation* on K is a map $v : K^\times \to \mathbb{R}$ satisfying:

1. $v(xy) = v(x) + v(y)$.
2. $v(x+y) \geqslant \min\{v(x), v(y)\}$

Remark 9. We usually define $v(0) = \infty$.

Given any exponential valuation v, we can define a multiplicative valuation by taking $|x| = c^{-v(x)}$ for some constant $c > 1$, and, conversely, given any multiplicative valuation, we can define an exponential valuation by taking $v(x) = -k\log(|x|)$ for some positive constant k. The constants are not important at this point since they account for equivalent valuations.

Definition 2.1.9. A valuation $|\cdot|$ (or a class of equivalent valuations) is *discrete* if the image of $K^\times$ is a discrete subgroup of $\mathbb{R}^+$.

Remark 10. For the non-archimedian case, this is equivalent to the fact that the corresponding exponential valuation v (which is defined up to a constant) is discrete, i.e. $v(K^\times)$ is a discrete subgroup of $\mathbb{R}$ and so $v(K^\times) = c\mathbb{Z}$ for some constant $c \in \mathbb{R}^+$. In this case, we say that the exponential valuation v is *normalized* if $v(K^\times) = \mathbb{Z}$.

Let $|\cdot|$ be a non-archimedian valuation on K. Then, from the property $|x+y| \leqslant \max\{|x|, |y|\}$, it follows that the set

$$A = \{x \in K : |x| \leqslant 1\}$$

is a subring of K. Moreover, A is a valuation ring (i.e. for any x in its field of fractions K, either $x \in A$ or $x^{-1} \in A$), and, consequently, a local ring. Its unique maximal ideal is

$$\mathfrak{p} = \{x \in K : |x| < 1\}$$

and the group of units is

$$A^\times = \{x \in K : |x| = 1\}\,.$$

The field $A/\mathfrak{p}$ is called the *residue class field* of A.

Since A is a valuation ring, it is integrally closed. To see it, let $x \in K$ be integral over A, i.e. there are coefficients $a_0, a_1, \ldots, a_{n-1} \in A$, of which we may assume $a_0 \neq 0$, such that $x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 = 0$. Suppose that $x \notin A$. Then, $x^{-1} \in A$, so that multiplying the previous relation by $x^{-(n-1)}$ and isolating the first term we get $x = -a_{n-1} - \cdots - a_1x^{-(n-2)} - a_0x^{-(n-1)}$, which contradicts $x \notin A$.

If the valuation is discrete, let v be the corresponding normalized exponential valuation, and take $\pi \in \mathfrak{p}$ such that $v(\pi) = 1$. Such an element is called a *local uniformizing parameter*. Then, $\mathfrak{p} = (\pi)$ and every ideal of A is generated by π^n for some $n \in \mathbb{N}$, so that A is principal and, since it is local, it is a discrete valuation ring. Moreover, every element of K can be written as $u\pi^n$ for some $u \in A^\times$ and some $n \in \mathbb{Z}$.

Proposition 2.1.10. Let K be a non-archimedian discrete valued field, let A be its valuation ring, let $\mathfrak{p}$ be its maximal ideal and let κ be its residue class field. Define $U^{(m)} = 1 + \mathfrak{p}^m$ for $m \geqslant 1$. Then, we have the following group isomorphisms:

$$A^\times / U^{(1)} \to \kappa^\times$$

and

$$U^{(m)} / U^{(m+1)} \to \kappa$$

for $m \geqslant 1$.

Proof. Let π be a local uniformizing parameter. It is straightforward that the maps

$$\begin{aligned} A^\times &\to \kappa^\times \\ a &\mapsto [a] \end{aligned}$$

and

$$\begin{aligned} U^{(m)} &\to \kappa \\ 1 + a\pi^m &\mapsto [a] \end{aligned}$$

for $m \geqslant 1$ induce the desired isomorphisms. □

2.2 Completions

References: [Neu99], [Mil17a]

Definition 2.2.1. A valued field $(K, |\cdot|)$ is *complete* if any Cauchy sequence of elements of K converges to an element of K.

Proposition 2.2.2. Let $(K, |\cdot|)$ be a valued field. Then, there is a complete valued field $(\hat{K}, |\cdot|)$ and a homomorphism $K \to \hat{K}$ preserving the valuation satisfying the following universal property: any homomorphism from $(K, |\cdot|)$ into a complete valued field $(L, |\cdot|')$ preserving the valuation can be uniquely extended to a continuous homomorphism $(\hat{K}, |\cdot|) \to (L, |\cdot|')$. The field $\hat{K}$ is uniquely determined up to isomorphism.

Proof. (Idea) The complete field $\hat{K}$ can be constructed by considering the set of all Cauchy sequences in K, defining an equivalence relation according to which two Cauchy sequences are equivalent if and only if their difference converges to zero, and taking the quotient set. This procedure is quite standard so we will not develop the details. □

Remark 11. The field $\hat{K}$ is called the *completion of K with respect to the valuation* $|\cdot|$.

Remark 12. Since the (topological) closure of K in $\hat{K}$ satisfies the same universal property, it must coincide with $\hat{K}$, which proves that K (i.e. its image in $\hat{K}$) is dense in $\hat{K}$.

Theorem 2.2.3. (Weak approximation theorem) Let $|\cdot|_1, ..., |\cdot|_n$ be inequivalent non-trivial valuations of K, let K_i be the completion of K with respect to $|\cdot|_i$, and let $\sigma_i : K \to K_i$ be the inclusions from the previous proposition. Then, the image of K under the map

$$\begin{aligned} K &\to \prod_{i=1}^{n} K_i \\ a &\mapsto (\sigma(a))_i \end{aligned}$$

is dense in $\prod_{i=1}^n K_i$ (with the product topology).

Proof. We begin by proving that, if $|\cdot|_1, ..., |\cdot|_n$ are inequivalent non-trivial valuations, there exists $z \in K$ such that

$$|z|_1 > 1 \text{ and } |z|_i < 1 \text{ for } i = 2, \dots, n\,.$$

We will argue by induction on n. For $n = 2$, observe that, as a consequence of Lemma 2.1.6, there exists $\alpha \in K$ such that $|\alpha|_1 < 1$ and $|\alpha|_2 \geqslant 1$, and there exists $\beta \in K$ such that $|\beta|_1 \geqslant 1$ and $|\beta|_2 < 1$. Therefore, for $z_2 = \beta/\alpha$, we have that $|z_2|_1 > 1$ and $|z_2|_2 < 1$.

Assume that we have found z_{n-1} such that

$$|z_{n-1}|_1 > 1 \text{ and } |z_{n-1}|_i < 1 \text{ for } i = 2, \dots, n-1\,.$$

By the same argument used for $n = 2$, there exists $y \in K$ such that $|y|_1 > 1$ and $|y|_n < 1$. If $|z_{n-1}|_n \leqslant 1$, then $z_n = z_{n-1}^m y$, where m is a positive integer, will satisfy the required property for sufficiently large m. Otherwise, if $|z_{n-1}|_n > 1$, we can take

$$z_n = \frac{z_{n-1}^m}{1 + z_{n-1}^m} y$$

with m sufficiently large.

Take $z \in K$ such that

$$|z|_1 > 1 \text{ and } |z|_i < 1 \text{ for } i = 2, \dots, n\,.$$

Then, the elements $z^m/(1 + z^m)$ get arbitrarily close to 1 with respect to $|\cdot|_1$ and arbitrarily close to zero with respect to $|\cdot|_i$ for $i = 2, \dots, n$ for m sufficiently large. In this way, for each of the valuations $|\cdot|_i$, with $1 \leqslant i \leqslant n$, we can find an element in K which is arbitrarily close to 1 with respect to this valuation and arbitrarily close to zero with respect to the other $n - 1$ given valuations.

Now, suppose that we are given some $(\alpha_i)_i \in \prod_{i=1}^n K_i$. Since K is dense in each K_i for each $i = 1, \dots, n$, we can find $a_i \in K$ arbitrarily close to α_i in K_i. Then, taking x_i to be arbitrarily close to 1 with respect to $|\cdot|_i$ and arbitrarily close to zero for the other valuations, we can get an element

$$x = x_1 a_1 + \cdots + x_n a_n$$

arbitrarily close to each a_i with respect to $|\cdot|_i$, and so we can get an element arbitrarily close to $(\alpha_i)_i$ in $\prod_{i=1}^n K_i$. □

Lemma 2.2.4. There is a unique valuation on $\mathbb{C}$ extending the classical absolute value of $\mathbb{R}$, and it is given by the classical absolute value on $\mathbb{C}$, i.e.

$$|a + bi| = \sqrt{a^2 + b^2}\,.$$

Proof. Let $|\cdot|$ be a valuation on $\mathbb{C}$ extending the classical absolute value of $\mathbb{R}$. Take $e^{2\pi q i}$, with $q \in \mathbb{Q}$. Then, there exists $n \in \mathbb{N}$ such that $(e^{2\pi q i})^n = 1$, so that $|e^{2\pi q i}|^n = 1$ and, consequently $|e^{2\pi q i}| = 1$. This allows to determine $|\cdot|$ over all elements $x \in \mathbb{C}$ of the form $x = re^{2\pi q i}$ with $q \in \mathbb{Q}$ and $r > 0$, and it is easy to check that the valuation coincides with the classical absolute value on these elements. Since

$$|a + bi| \leqslant |a| + |bi| = |a| + |b|\,,$$

these elements form a dense subset of $\mathbb{C}$ and so determine $|\cdot|$. □

Theorem 2.2.5. Let K be a field, and assume that it is complete with respect to an archimedian valuation $|\cdot|$. Then, there is an isomorphism σ between K and either $\mathbb{R}$ or $\mathbb{C}$ such that

$$|\alpha| = |\sigma\alpha|^c \text{ for all } \alpha \in K$$

for some constant $0 < c \leqslant 1$ (on the right hand side $|\cdot|$ denotes the classical absolute value on $\mathbb{R}$ or $\mathbb{C}$).

Proof. We may assume that $\mathbb{R} \subseteq K$. To prove it, observe that, since K has an archimedian valuation, it has characteristic zero and therefore it contains a subfield isomorphic to $\mathbb{Q}$, and which we can consider to be $\mathbb{Q}$. The restriction of $|\cdot|$ to $\mathbb{Q}$ is an archimedian valuation on $\mathbb{Q}$ and is therefore equivalent to the classical absolute value on $\mathbb{Q}$. Then, because of the uniqueness of completions, the topological closure of $\mathbb{Q}$ in K is isomorphic to $\mathbb{R}$ through an isomorphism preserving the valuations.

Let $\xi \in K$, and consider the continuous function

$$\begin{aligned} f : \mathbb{C} &\to \mathbb{R} \\ z &\mapsto |\xi^2 + (z + \overline{z})\xi + z\overline{z}| \,, \end{aligned}$$

where $\overline{z}$ denotes the complex conjugate of z (observe that both $z + \overline{z}$ and $z\overline{z}$ are real). Since $\lim_{|z|\to\infty} f(z) = \infty$, the function f has a minimum, which we denote by m.

Assume that $m > 0$. The set $S = f^{-1}(m)$ is bounded and closed, so that there exists some $z_0 \in S$ such that $|z_0| \geqslant |z|$ for all $z \in S$. Take some $\epsilon \in \mathbb{R}$ such that $0 < \epsilon < m$ and consider the polynomial

$$g(X) = X^2 + (z_0 + \overline{z_0})X + z_0\overline{z_0} + \epsilon \,.$$

Let $z_1, \overline{z_1} \in \mathbb{C}$ be the roots of this polynomial. Then $z_1\overline{z_1} = z_0\overline{z_0} + \epsilon$, so that $|z_1| > |z_0|$ and $f(z_1) > m$. Now, for a positive integer n, define the polynomial

$$G(X) = (g(X) - \epsilon)^n - (-\epsilon)^n = \prod_{i=1}^{2n}(X - \alpha_i) = \prod_{i=1}^{2n}(X - \overline{\alpha_i}) \,.$$

Clearly z_1 is a root of $G(X)$; we will assume $\alpha_1 = z_1$. Substituting ξ in

$$G(X)^2 = \prod_{i=1}^{2n}(X^2 + (\alpha_i + \overline{\alpha_i})X + \alpha_i\overline{\alpha_i})$$

we get

$$|G(\xi)|^2 = \prod_{i=1}^{2n} f(\alpha_i) \geqslant f(z_1)m^{2n-1} \,.$$

On the other hand

$$|G(\xi)| \leqslant |g(\xi) - \epsilon|^n + |-\epsilon|^n = f(z_0)^n + \epsilon^n = m^n + \epsilon^n \,.$$

Combining both inequalities we get

$$\frac{f(z_1)}{m} \leqslant \left(1 + \left(\frac{\epsilon}{m}\right)^n\right)^2 \,,$$

and, letting $n \to \infty$, we deduce that $f(z_1) \leqslant m$, which is a contradiction.

Therefore $m = 0$, which shows that ξ is algebraic over $\mathbb{R}$. Hence, we see that all elements in K are algebraic over $\mathbb{R}$ and consequently that K is isomorphic to either $\mathbb{R}$ or $\mathbb{C}$, and the condition on the valuations for this isomorphism follows from Lemma 2.2.4. □

Let K be a non-archimedian valued field and let $\hat{K}$ be its completion. Then, any element of $\hat{K}$ can be written as the limit of a Cauchy sequence of elements of K. Let $a \in \hat{K}$, $a = \lim_n a_n$, $a_n \in K$. Then,

$$|a| = \lim_n |a_n| .$$

If $a \neq 0$, the sequence $(|a_n|)_n$ becomes eventually stationary. To prove it, observe that, since the sequence $(a_n)_n$ converges, there exists $n_0 \in \mathbb{N}$ such that $|a_n - a| < |a|$ for all $n \geqslant n_0$, so that

$$|a_n| = |a + a_n - a| = \max\{|a|, |a_n - a|\} = |a| .$$

This fact proves that the possible values taken by the non-archimedian valuation on the completion are those taken by the original valuation on K. In particular, if the original valuation on K is discrete, its extension to the completion is also discrete.

Another consequence is that the valuation ring

$$\hat{A} = \{x \in \hat{K} : |x| \leqslant 1\}$$

and the maximal ideal

$$\hat{\mathfrak{p}} = \{x \in \hat{K} : |x| < 1\}$$

can be regarded as the set of limits of Cauchy sequences in A and $\mathfrak{p}$, respectively.

Proposition 2.2.6. Let K be a field with a non-archimedian valuation. Let $\hat{K}$ be its completion, let A and $\hat{A}$ be the corresponding valuation rings and let $\mathfrak{p}$ and $\hat{\mathfrak{p}}$ be the corresponding maximal ideals. Then,

$$\hat{A}/\hat{\mathfrak{p}} \simeq A/\mathfrak{p} .$$

Moreover, if the valuation is discrete,

$$\hat{A}/\hat{\mathfrak{p}}^n \simeq A/\mathfrak{p}^n$$

for all $n \in \mathbb{N}$.

Proof. Consider the natural map

$$A \to \hat{A}/\hat{\mathfrak{p}} .$$

Its kernel is $\hat{\mathfrak{p}} \cap A = \mathfrak{p}$. Moreover, the map is surjective, since, given any element $\alpha \in \hat{A}$, we can find an element $a \in A$ which is arbitrarily close to α; in particular, we can find a such that $\alpha - a \in \hat{\mathfrak{p}}$. Therefore, we get an isomorphism

$$A/\mathfrak{p} \to \hat{A}/\hat{\mathfrak{p}} .$$

If the valuation is discrete, let π be a local uniformizing parameter of A. Taking into account the discussion previous to this proposition, we see that π is also a local uniformizing parameter for $\hat{A}$, which is also a discrete valuation ring, and

$$\hat{\mathfrak{p}}^n = \{x \in \hat{A} : |x| \leqslant |\pi|^n\} .$$

Therefore, the natural map

$$A \to \hat{A}/\hat{\mathfrak{p}}^n$$

has kernel $\hat{\mathfrak{p}}^n \cap A = \mathfrak{p}^n$ and is surjective since, for any $\alpha \in \hat{A}$, we can find $a \in A$ such that $|\alpha - a| \leqslant |\pi|^n$. □

Lemma 2.2.7. Let K be a complete non-archimedian discrete valued field, π a local uniformizing parametre and S a set of representatives of the residue class field. Then, any element of K can be uniquely written as the limit of a series of the form

$$\pi^r \left(a_0 + a_1\pi + a_2\pi^2 + \cdots\right)$$

with $r \in \mathbb{Z}$, $a_i \in S$ for all $i \in \mathbb{N}$, $a_0 \neq 0$ in the residue class field.

Proof. First we prove that such a series converges and so represents an element in K. Since K is complete, we need only prove that it is Cauchy. Let

$$\alpha_n = \pi^r(a_0 + a_1\pi + \cdots + a_n\pi^n)$$

for $n \in \mathbb{N}$. Then, for $n, m \in \mathbb{N}$, with $m > n$,

$$\alpha_m - \alpha_n = \pi^r(a_{n+1}\pi^{n+1} + \cdots + a_m\pi^m)\,,$$

and, applying the strong triangle inequality,

$$|\alpha_m - \alpha_n| \leqslant |\pi|^{r+n+1}\,.$$

which obviously tends to zero as both m and n tend to infinity.

Let A be the valuation ring of K, and let κ be the residue class field. Take any $\alpha \in K$. It can be written uniquely as $\alpha = u\pi^r$, where $u \in A^\times$. Let $a_0 \in S$ be the representative of the class of u in κ. Then, we have $u - a_0 \in (\pi)$, so that we can write $u - a_0 = v_1\pi$, with $v_1 \in A$. Let $a_1 \in S$ be the representative of the class of v_1 in κ. Then, we have $v_1 - a_1 \in (\pi)$, so that we can write $v_1 - a_1 = v_2\pi$, with $\pi \in A$, and we have

$$\alpha = \pi^r(a_0 + v_1\pi) = \pi^r(a_0 + a_1\pi + v_2\pi^2)\,.$$

Continuing in this way, we get a sequence $(a_n)_n$, with $a_n \in S$ for all n and a_0 different from zero in κ, and a sequence $(v_n)_n$, with $v_n \in A$ for all n, such that,

$$\alpha = \pi^r(a_0 + a_1\pi + \cdots + a_n\pi^n + v_{n+1}\pi^{n+1})\,,$$

so that the sequence

$$\alpha_n = \pi^r(a_0 + a_1\pi + \cdots + a_n\pi^n)$$

clearly converges to α.

Now, assume that two such sequences represent the same $\alpha \in K$, i.e. we have

$$\pi^r(a_0 + a_1\pi + \cdots) = \pi^s(b_0 + b_1\pi + \cdots)\,.$$

The exponents r and s are determined by $|\alpha|$, so that $r = s$. Suppose that the sequences $(a_n)_n$ and $(b_n)_n$ are not equal, and let k be the minimum natural number such that $a_k \neq b_k$. Since $a_k, b_k \in S$, and S is a set of representatives of κ (i.e. it has an unique representative for each class in κ), $a_k - b_k \notin (\pi)$. Then, if we define

$$\alpha_n = \pi^r(a_0 + a_1\pi + \cdots + a_n\pi^n)$$

and

$$\beta_n = \pi^r(b_0 + b_1\pi + \cdots + b_n\pi^n)\,.$$

we see that, for all $n \geqslant k$,

$$|\alpha_n - \beta_n| = |\pi^r((a_k - b_k)\pi^k + (a_{k+1} - b_{k+1})\pi^{k+1} + \cdots + (a_n - b_n)\pi^n)| = |\pi|^{r+k}\,,$$

which contradicts the fact that both $(\alpha_n)_n$ and $(\beta_n)_n$ tend to α. □

Definition 2.2.8. Let A be the valuation ring of a non-archimedian valued field. A polynomial $f(X) \in A[X]$, $f(X) = a_0 + a_1X + \cdots a_nX^n$ is primitive if

$$|f| = \max\{|a_0|, |a_1|, \ldots, |a_n|\} = 1\,.$$

Proposition 2.2.9. (Hensel's lemma) Let K be a complete non-archimedian discrete valued field, A its valuation ring, $\mathfrak{p}$ its maximal ideal and κ its residue class field. Let $f \in A[X]$ be a primitive polynomial. If f admits a factorization in κ

$$\overline{f}(X) = g_*(X)h_*(X)$$

into relatively prime polynomials $g_*(X), h_*(X) \in \kappa[X]$, then there exist $g(X), h(X) \in A[X]$ with $\deg(g) = \deg(g_*)$ such that $\overline{g}(X) = g_*(X)$, $\overline{h}(X) = h_*(X)$ and $f(X) = g(X)h(X)$.

Proof. Let $d = \deg(f)$ and $m = \deg(g_*)$ (observe that, since f is primitive, g_* and h_* are not zero). Then $\deg(h_*) \leqslant d - m$. Take polynomials $g_0, h_0 \in A[X]$ such that $\overline{g_0} = g_*$, $\overline{h_0} = h_*$ and $\deg(g_0) = m$. For these polynomials, clearly $f \equiv g_0h_0 \pmod{\mathfrak{p}}$. We will find sequences of polynomials $(p_n)_{n\geqslant 1}$ and $(q_n)_{n\geqslant 1}$, with $p_n, q_n \in A[X]$, $\deg(p_n) < m$ and $\deg(q_n) \leqslant d - m$ for all $n \geqslant 1$, such that, for all $n \geqslant 0$, the polynomials

$$g_n = g_0 + \pi p_1 + \pi^2 p_2 + \cdots \pi^n p_n$$
$$h_n = g_0 + \pi q_1 + \pi^2 q_2 + \cdots \pi^n q_n$$

satisfy that $f \equiv g_nh_n \pmod{\mathfrak{p}^{n+1}}$. Then, taking

$$g = g_0 + \pi p_1 + \pi^2 p_2 + \cdots$$
$$h = g_0 + \pi q_1 + \pi^2 q_2 + \cdots\,,$$

we will obviously have $f = gh$, with $\overline{g}(X) = g_*(X)$, $\overline{h}(X) = h_*(X)$ and $\deg(g) = \deg(g_*)$.

Let us see how to find p_n and q_n once g_{n-1} and h_{n-1} are already determined. We want to find polynomials p_n and q_n such that

$$(g_{n-1} + \pi^n p_n)(h_{n-1} + \pi^n q_n) \equiv f \pmod{\mathfrak{p}^{n+1}}$$

or, equivalently,

$$f - g_{n-1}h_{n-1} \equiv (g_{n-1}q_n + h_{n-1}p_n)\pi^n \pmod{\mathfrak{p}^{n+1}}\,.$$

Since $f - g_{n-1}h_{n-1} \equiv 0 \pmod{\mathfrak{p}^n}$, dividing by π^n we obtain

$$f_n \equiv g_{n-1}q_n + h_{n-1}p_n \equiv g_0q_n + h_0p_n \pmod{\mathfrak{p}}\,,$$

where $f_n = \pi^{-n}(f - g_{n-1}h_{n-1})$. Since g_* and h_* are relatively prime, there exist polynomials $a, b \in A[X]$ such that $ag_0 + bh_0 \equiv 1 \pmod{\mathfrak{p}}$. Let

$$b(X)f_n(X) = q(X)g_0(X) + r(X)\,,$$

with $\deg(r) < \deg(g_0) = m$. Observe that, since $\deg(g_0) = \deg(g_*)$ and $\overline{g_0} = g_*$, the leading coefficient of g_0 is a unit and, consequently, $q(X) \in A[X]$ and $r(X) \in A[X]$. We have

$$f_n \equiv (ag_0 + bh_0)f_n = (af_n + qh_0)g_0 + rh_0 \pmod{\mathfrak{p}}\,.$$

Take $p_n = r$ and let q_n be the polynomial obtained from $af_n + qh_0$ by eliminating all coefficients lying in $\mathfrak{p}$. Clearly $\deg(p_n) < m$ and, since $\deg(f_n) \leqslant d$, $\deg(g_0) = m$ and $\deg(rh_0) < m+d-m = d$, we deduce that $\deg(q_n) \leqslant d - m$. □

Corollary 2.2.10. Let K be a complete non-archimedian discrete valued field and let $f(X) = a_0 + a_1X + \cdots a_nX^n \in K[X]$ be an irreducible polynomial, with $a_n \neq 0$. Then

$$|f| = \max\{|a_0|, |a_n|\}\,.$$

Proof. Let A be the valuation ring of K and let $\mathfrak{p}$ be its maximal ideal. Multiplying $f(X)$ by a suitable constant in $K^\times$, we may assume that $f(X) \in A[X]$ and $|f| = 1$. Let us define $r = \min\{k : |a_k| = 1\}$. Then

$$f(X) \equiv X^r(a_r + a_{r+1}X + \cdots a_nX^n) \pmod{\mathfrak{p}}\,,$$

which, if $0 < r < n$, would contradict the previous proposition. □

Lemma 2.2.11. Let K be a complete non-archimedian valued field, and let V be an n-dimensional normed K-vector space. Then, for any basis $v_1, \ldots, v_n$ of V, the maximum norm

$$\|x_1v_1 + \cdots x_nv_n\| = \max\{|x_1|, \ldots, |x_n|\}$$

is equivalent to the given norm on V.

Proof. Let $|\cdot|$ be the given norm on V. Let $v_1, \ldots, v_n$ be a basis of V and let $\|\cdot\|$ be the corresponding maximum norm. We need to find constants $\rho, \rho' \in \mathbb{R}^+$ such that for all $v \in V$

$$\rho\|v\| \leqslant |v| \leqslant \rho'\|v\|\,.$$

If $v = x_1v_1 + \cdots + x_nv_n$, then

$$|v| \leqslant |x_1||v_1| + \cdots + |x_n||v_n|\,,$$

so we may obviously take $\rho' = |v_1| + \cdots |v_n|$.

For ρ, let us argue by induction on n. For $n = 1$ we can simply take $\rho = |v_1|$. Assume that the result has been proved for $k < n$. Then for each of the subspaces

$$V_i = \langle v_1, \ldots, v_{i-1}, v_{i+1}, \ldots, v_n\rangle$$

the restriction of $|\cdot|$ is equivalent to the norm of the maximum defined, for example, for the basis $v_1, \ldots, v_{i-1}, v_{i+1}, \ldots, v_n$. In particular, we deduce that each of the subspaces V_i is complete and hence closed, and that so is $v_i + V_i$. Hence the subset

$$W = \bigcap_{i=1}^{n} (v_i + V_i)$$

is closed, and, since $0 \notin W$, there is some $\rho > 0$ such that $B(0, \rho) \cap W = \emptyset$, i.e. such that $|v_i + w_i| \geqslant \rho$ for all $w_i \in V_i$ and for all $i = 1, \ldots, n$. Therefore, for each $x \in V$ with $x = x_1v_1 + \cdots + x_nv_n$ and $x \neq 0$, if $|x_r| = \max\{|x_i| : i = 1, \ldots, n\}$, then

$$|v| = \|v\||x_r^{-1}v| = \left|\frac{x_1}{x_r}v_1 + \cdots + v_r + \cdots + \frac{x_n}{x_r}\right| \geqslant \rho\|v\|\,.$$

□

Proposition 2.2.12. Let $(K, |\cdot|)$ be a complete valued field, and let L be an algebraic extension of K. Then, there is a unique extension of $|\cdot|$ to a valuation in L. For a finite extension L/K of degree n, the extension of the valuation is given by the formula

$$|\alpha| = \sqrt[n]{|\mathrm{Nm}_{L/K}(\alpha)|}$$

and L is also complete with respect to this valuation.

Proof. If the valuation is archimedian, we already know by Theorem 2.2.5 that K is isomorphic to either $\mathbb{R}$ or $\mathbb{C}$, so we need only check the case $K = \mathbb{R}$, $L = \mathbb{C}$. By Theorem 2.2.5, all archimedian valuations on $\mathbb{R}$ are given by $|x| = |x|_\infty^c$, where $|\cdot|_\infty$ is the classical absolute value and $0 < c \leqslant 1$. Following the proof of Lemma 2.2.4, such a valuation extends uniquely to $\mathbb{C}$ as

$$|\alpha| = \sqrt{|\mathrm{Nm}_{\mathbb{C}/\mathbb{R}}(\alpha)|}\,.$$

Now, let us focus on the non-archimedian case. If the valuation is trivial, the only extension is clearly the trivial valuation of L, so we will also assume that the given valuation is non-trivial. It is enough to prove the theorem for finite extensions, so we will consider that L/K is finite of degree n. Let A be the valuation ring of K and let B be its integral closure in L. Then, we first claim that

$$B = \{x \in L : \mathrm{Nm}_{L/K}(x) \in A\}\,.$$

Since A is integrally closed, the inclusion $\subseteq$ is clear. For the inclusion $\supseteq$, let $x \in L$ satisfy $\mathrm{Nm}_{L/K}(x) \in A$, and let $f(X) = X^m + a_{m-1}X^{m-1} + \cdots + a_1X + a_0 \in K[X]$ be the minimal polynomial of x over K. Since $\mathrm{Nm}_{L/K}(x) = (-1)^n a_0^{n/m}$, we see that $|a_0| \leqslant 1$. Then, by Corollary 2.2.10, $|a_i| \leqslant 1$ for all the coeficients of $f(X)$, which implies $f(X) \in A[X]$ and so $x \in B$.

Now, we will check that the formula

$$|\alpha| = \sqrt[n]{|\mathrm{Nm}_{L/K}(\alpha)|}$$

defines a valuation on L. The conditions $|x| \geqslant 0$, $|x| = 0 \Leftrightarrow x = 0$ and $|xy| = |x||y|$ are clearly satisfied. We claim that the condition

$$|x + y| \leqslant \max\{|x|, |y|\}$$

is equivalent to the condition

$$|x| \leqslant 1 \Rightarrow |x + 1| \leqslant 1\,.$$

It is clear that the former condition implies the latter. For the converse, divide $x + y$ by x or y (the one with greater valuation). Now, the last condition holds since

$$|x| \leqslant 1 \Leftrightarrow |\mathrm{Nm}_{L/K}(x)| \leqslant 1 \Leftrightarrow \mathrm{Nm}_{L/K}(x) \in A \Leftrightarrow x \in B$$

and clearly $x \in B \Rightarrow x + 1 \in B$.

To prove uniqueness, suppose that we have a second valuation $|\cdot|'$ on L extending the original valuation on K. Let B' be the corresponding valuation ring, and $\mathfrak{P}'$ the corresponding maximal ideal. We first prove that $B \subseteq B'$. Assume $x \in B \setminus B'$. Then, x satisfies a relation of the form $x^m + a_{m-1}x^{m-1} + \cdots a_1x + a_0 = 0$, where $a_i \in A$ for all i and we may assume $a_0 \neq 0$. Since $x \notin B'$, $|x|' < 1$, so that $x^{-1} \in \mathfrak{P}'$. Thus, multiplying the previous relation by x^{-m} we get $1 = -a_{m-1}x^{-1} - \cdots - a_1x^{-(m-1)} - a_0x^{-m} \in \mathfrak{P}'$, which is a contradiction.

Therefore, we have proved that $B \subseteq B'$, or, equivalently,

$$|x| \leqslant 1 \Rightarrow |x|' \leqslant 1\,.$$

This implies that both valuations are equivalent, as otherwise, by the weak approximation theorem, we could find some $x \in L$ such that $|x| \leqslant 1$ but $|x|' > 1$.

The fact that L is complete with respect to the extended valuation is a consequence of the previous lemma. □

Definition 2.2.13. Let K be a non-archimedian valued field, with exponential valuation v, and let L be an algebraic extension of K with exponenial valuation w extending v. Let κ and λ_w be the residue class fields of K and L, respectively. Then, the *ramification index* and the *inertia degree* of the extension $w|v$ are defined as

$$e_w = [w(L^\times) : v(K^\times)]$$

and

$$f_w = [\lambda_w : \kappa]\,,$$

respectively.

If K is complete with respect to the valuation v, there is a unique extension w of v to an algebraic extension L of K. In this case, we will often refer to e_w and f_w as the ramification index and inertia degree of the extension L/K.

Proposition 2.2.14. Let K be a complete non-archimedian valued field with exponential valuation v, let L be a finite extension of K and let w be the unique extension of v to L. Let e and f be the ramification index and the inertial degree, respectively, of the extension $w|v$. Then,

$$[L : K] \geqslant ef\,.$$

Moreover, if v is discrete and the extension L/K is separable, we have in fact

$$[L : K] = ef\,.$$

Proof. Let A be the valuation ring of K, let $\mathfrak{p}$ be its maximal ideal and let κ be its residue class field. Let B be the valuation ring of L, let $\mathfrak{P}$ be its maximal ideal and let λ be its residue class field. Let $\{\alpha_i\}_{i\in I}$ be a set of representatives of a basis of λ over κ, and let $\{\beta_j\}_{j\in J}$ be a set of elements in $L^\times$ such that $\{w(\beta_j)\}_{j\in J}$ forms a set of representatives of $w(L^\times)/v(K^\times)$. We claim that the elements $\alpha_i\beta_j$, with $i \in I$ and $j \in J$, are linearly independent over K. Assume that there is some non-trivial linear combination of this elements which equals zero. We may write such a combination as

$$\sum_{r=1}^{N}\sum_{s=1}^{M} x_{i_r j_s}\alpha_{i_r}\beta_{j_s}\,.$$

where $x_{i_r j_s} \in K$ for all r, s. Define

$$y_{j_s} = \sum_{r=1}^{N} x_{i_r j_s}\alpha_{i_r}\,,$$

for $s = 1, \ldots, M$. If $y_{j_s} \neq 0$, we can divide both sides of the previous expression by a coefficient $x_{i_r j_s}$ with minimum exponential valuation $v(x_{i_r j_s})$, so that we get at the right a linear combination of the elements α_{i_r} with coefficients in A and one of them equal to 1. Since these elements are linearly independent over κ when considered in λ, this linear combination cannot be in $\mathfrak{P}$, i.e. it must be a unit. This proves that the exponential valuation $w(y_{j_s})$ equals the valuation of a coefficient $x_{i_r j_s}$ with minimum exponential valuation, and, hence, $w(y_{j_s}) \in v(K^\times)$. Note also that there must be some $y_{j_s} \neq 0$, as by assumption not all the coefficients $x_{i_r j_s}$ are zero and the α_{i_r} are linearly independent. Therefore, in order that the sum

$$\sum_{s=1}^{M} y_{j_s} \beta_{j_s}$$

be equal to zero, there must be two non-zero terms with the same valuation, i.e. there exist $r \neq s$, with $1 \leqslant r, s \leqslant M$, such that $w(y_{j_r}\beta_{j_r}) = w(y_{j_s}\beta_{j_s}) \neq \infty$. But, since in this case $w(y_{j_r}), w(y_{j_s}) \in v(K^\times)$, we would obtain $w(\beta_{j_r}) - w(\beta_{j_s}) \in v(K^\times)$, which is a contradiction. Therefore, we deduce that

$$[L : K] \geqslant ef\,.$$

Now, assume that the extension L/K is separable and the valuation v is discrete. Since the valuation w is given by the formula

$$w(\alpha) = \frac{1}{n} v(\mathrm{Nm}_{L/K})\,,$$

where $n = [L : K]$, it is also discrete. Let Π be a local uniformizing parameter of L. Then, we can take $\beta_i = \Pi^i$, for $i = 0, 1, \ldots, e-1$. Take also $\alpha_1, \ldots, \alpha_f$ to be representatives of a basis of λ over κ. Define

$$M = \sum_{i=0}^{e-1} \sum_{j=1}^{f} A\alpha_j \Pi^i\,,$$

which is clearly an A-submodule of B. We claim that $M = B$. Consider the A-submodule

$$N = \sum_{j=1}^{f} A\alpha_j\,.$$

Then, since the elements $\alpha_1, \ldots, \alpha_f$ form a basis of $B/\Pi B$ over $A/\Pi^e A$, we have that

$$B = N + \Pi B\,.$$

Therefore,

$$B = N + \Pi(N + \Pi B) = \cdots = N + \Pi N + \cdots + \Pi^{e-1} N + \Pi^e B = M + \mathfrak{p}B\,.$$

We saw in the proof of the previous proposition that B is the integral closure of A in L. Therefore, since L/K is separable and A is a discrete valuation ring (and, *a fortiori*, it is a principal ideal domain), we know that B is a free A-module of rank n. Since A is a local ring with maximal ideal $\mathfrak{p}$, application of Nakayama's lemma to the identity

$$B = M + \mathfrak{p}B$$

yields $B = M$, and, since it has rank n as an A-module, we get, in this case,

$$[L : K] = ef\,.$$

□

Remark 13. In fact, the proposition also holds for an algebraic extension L/K in general, either finite or infinite, with the obvious conventions. For the first part of the proposition, the one concerning the inequality $[L : K] \geqslant ef$, the given proof is clearly also valid if L/K is infinite. For the second part, concerning the equality $[L : K] = ef$ when L/K is separable, observe that, if L/K is infinite, there exist finite subextensions of arbitrarily large degree.

2.3 Local fields

References: [Neu99], [Mil17a], [Mil13]

Definition 2.3.1. A *local field* is a field provided with a non-trivial valuation which is locally compact with the topology induced by the valuation.

Remark 14. A local field is complete. To prove it, let T be a compact neighborhood of 1. Let $B(1, \delta) \subseteq T$. Let $(a_n)_n$ be a Cauchy sequence not converging to 0. Hence, there exists $\epsilon_0 > 0$ such that $|a_n| \geqslant \epsilon_0$ for infinitely many $n \in \mathbb{N}$, which, taking into account the fact that the sequence is Cauchy, implies that there exist some ϵ_1 and some $n_1 \in \mathbb{N}$ such that, for all $n \geqslant n_1$, $|a_n| \geqslant \epsilon_1$. Now, using again the fact that the sequence is Cauchy, there exists some $n_2 \in \mathbb{N}$ such that, for all $n, m \geqslant n_2$, $|a_n - a_m| < \delta\epsilon_1$. We may assume $n_2 \geqslant n_0$. Then, $a_{n_2} \neq 0$ and, multiplying the sequence by $a_{n_2}^{-1}$, we get a Cauchy sequence $(b_n)_n$ such that, for all $n \geqslant n_2$, $b_n \in B(1, \delta) \subseteq T$. Thus, $(b_n)_n$ is convergent, and, consequently, $(a_n)_n$ is convergent too.

Remark 15. Taking into account the previous remark and Theorem 2.2.5, we easily see that, up to isomorphism, there are only two archimedian local fields: $\mathbb{R}$ and $\mathbb{C}$.

Proposition 2.3.2. A non-archimedian valued field K is a local field if and only it is complete, the valuation is discrete and the residue class field is finite.

Proof. Let A be the valuation ring of K and $\mathfrak{p}$ its maximal ideal.

Suppose that K is a local field. Then, there is a compact neighborhood of 0. This neighborhood must contain some subset of the form dA for some $d \in K^\times$. As such a subset is clearly closed, it is also compact, and, since multiplication by d is a homeomorphism, this implies that A is compact. From the strong triangle inequality, it follows that the maximal ideal $\mathfrak{p}$ of A is closed, so that, since it is contained in A, it is also compact. Since the valuation is a continuous map from K to $\mathbb{R}$, the image of $\mathfrak{p}$ under the valuation map must be a compact subset of $[0, 1)$, which implies that it is discrete (otherwise its image would be dense in $[0, 1)$), and hence the valuation is discrete. Finally, since A is compact and, for a set of representatives S of the residue class field, $A = \bigsqcup_{s \in S}(s + \mathfrak{p})$, where the sets $s + \mathfrak{p}$ are clearly open, we deduce that the residue class field is finite.

For the converse, we need only prove that A is compact, because this already implies that K is locally compact. Since A is a metric space, we may prove compactness by showing that it is complete and totally bounded (i.e. for any $\delta > 0$, there is a finite covering of A comprised of open balls of radius δ). Completeness is assumed, and totally boundedness follows easily from the finiteness of the residue class field if we think of the expansion of any element in terms of the powers of a local uniformizing parameter (Lemma 2.2.7). □

Proposition 2.3.3. Every non-archimedian local field K is isomorphic to either a finite extension of $\mathbb{Q}_p$, if $\mathrm{char}K = 0$, or to a finite extension of $\mathbb{F}_p((t))$, if $\mathrm{char}K = p$.

Proof. Observe that any finite extension of either $\mathbb{Q}_p$ or $\mathbb{F}_p((t))$ is an archimedian local field. In fact, for any such field, the valuation is discrete and the residue class field is finite, both

facts because of Proposition 2.2.14, and we also know that such a field is complete because of Proposition 2.2.12.

Let K be a local field. Assume, first, that $\mathrm{char}K = 0$. Then, it contains a subfield isomorphic to $\mathbb{Q}$. By the Ostrowski theorem, the restricion to this subfield of the non-trivial non-archimedian valuation of K must be equivalent to a p-adic valuation $|\cdot|_p$. Since K is complete, it therefore contains a subfield isomorphic to $\mathbb{Q}_p$. Since The valuation of K is discrete, the ramification index of the extension $K/\mathbb{Q}_p$ is finite, and, since the residue class field of K is finite, the inertia degree f of the extension $K/\mathbb{Q}_p$ is also finite. Therefore, because of the remark following Proposition 2.2.14, $[K : \mathbb{Q}_p] = ef$ is finite ($K/\mathbb{Q}_p$ is separable as $\mathrm{char}\mathbb{Q}_p = 0$), which shows that K is a finite extension of $\mathbb{Q}_p$.

Now, assume that $\mathrm{char}K = p$ for some prime p. In this case, K contains $\mathbb{F}_p$ as a subfield, and the residue class field κ is a finite extension of $\mathbb{F}_p$. Let $\kappa = \mathbb{F}_p(\alpha)$. Let $f = [\kappa : \mathbb{F}_p]$. Then, the field κ consists of the roots of the polynomial $X^{p^f} - X \in \mathbb{F}_p[X]$. Therefore, this polynomial splits completely into linear factors in $\kappa[X]$, and, by Hensel's lemma, so it does in $K[X]$, which allows us to see κ as a subfield of K. Finally, if t is a local uniformizing parameter of K, Lemma 2.2.7 shows that $K = \kappa((t))$. □

Proposition 2.3.4. Let K be a non-archimedian local field, with residue class field κ and maximal ideal $\mathfrak{p}$. Let $q = |\kappa|$, let μ_{q-1} denote the $q-1$-roots of unity of K, let π be a local uniformizing parameter and let $U^{(1)} = 1 + \mathfrak{p}$. Then, for its multiplicative group $K^\times$, we have the following decomposition:

$$K^\times = \pi^{\mathbb{Z}} \times \mu_{q-1} \times U^{(1)} .$$

Proof. Let A be the valuation ring of K. Since K is a discrete non-archmedian valued field, every element $\alpha \in K^\times$ can be uniquely written in the form $\alpha = u\pi^r$, where $r \in \mathbb{Z}$ and $u \in A^\times$. This proves that $K^\times = \pi^{\mathbb{Z}} \times A^\times$.

Consider the quotient map

$$A^\times \to \kappa^\times .$$

Clearly, its kernel is $U^{(1)} = 1 + \mathfrak{p}$, so that the exact sequence

$$0 \longrightarrow U^{(1)} \longrightarrow A^\times \longrightarrow \kappa^\times \longrightarrow 0$$

is obtained. Since $X^{q-1} - 1$ splits completely into linear factors in κ, by Hensel's lemma so it does in $K^\times$, which proves that the quotient $A^\times \to \kappa^\times$ maps μ_{q-1} bijectively onto $\kappa^\times$, and we get a section for the previous exact sequence. Hence,

$$A^\times = \mu_{q-1} \times U^{(1)} .$$

□

The finite extensions of $\mathbb{Q}_p$ are often refered to as p-adic number fields.

Lemma 2.3.5. Let K be a p-adic number field. There exists a unique continuous homomorphism

$$\log_p : K^\times \to K$$

such that $\log_p(p) = 0$ and, for all $1 + x \in U^{(1)}$,

$$\log_p(1 + x) = x - \frac{x^2}{2} + \frac{x^3}{3} - \cdots .$$

This function is called *p-adic logarithm.*

Proof. First of all, let us check that, for $1+x \in U^{(1)}$, the sum of the series defining $\log(x)$ actually converges. We can consider in K the exponential valuation extending the exponential valuation v_p of $\mathbb{Q}_p$, which we will also denote by v_p. Then, for any positive integer k we have

$$v_p(k) \leqslant \frac{\log k}{\log p}\,.$$

Therefore, we have

$$v_p\left(\frac{x^k}{k}\right) = kv_p(x) - v_p(k) \geqslant kv_p(x) - \frac{\log k}{\log p} = \log k\left(v_p(x)\frac{k}{\log k} - \frac{1}{\log p}\right)\,,$$

so that, if $1+x \in U^{(1)}$ and, consequently, $v_p(x) > 0$, we see that the sequence $v_p(x^n/n)$ and, hence, that the sequence x^n/n has limit zero. Because of the strong inequality and the fact that K is complete, this is enough to ensure that the series defining $\log(1+x)$ converges (absolutely).

Also, observe that, for any $1+x, 1+y \in U^{(1)}$,

$$\log_p((1+x)(1+y)) = \log(1+x) + \log(1+y)\,,$$

as the series at each side agree as formal power series in x and y and we have absolute convergence.

Let κ be the residue class field of K, let $q = |\kappa|$, let μ_{q-1} be the subgroup of $q-1$-th roots of unity in K, and let π be a local uniformizing parameter. Let e be the ramification index of $K/\mathbb{Q}_p$, so that $(p) = (\pi^e)$. Because of the previous proposition, every element $a \in K$ can be written uniquely in the form

$$a = \pi^r \mu(a) u(a)\,,$$

where $r \in \mathbb{Z}$ and $\mu(a) \in \mu_{q-1}$ and $\quad u(a) \in U^{(1)}$, being q the number of elements in the residue class field κ. Observe that, if $\xi \in \mu_{q-1}$, then we must have

$$\log_p(\xi) = \frac{1}{q-1}\log_p(\xi^{q-1}) = \frac{1}{q-1}\log_p(1) = 0\,.$$

On the other hand,

$$0 = \log_p(p) = \log_p(\pi^e u(p)) = e\log_p(\pi) + \log_p(u(p))\,,$$

so that we must have

$$\log_p(\pi) = -\frac{1}{e}\log_p(u(p))\,.$$

Altogether, we conclude that the only 'candidate' function that could meet the conditions in the statement is given by

$$\log_p(a) = \log_p(u(a)) - \frac{v_{\mathfrak{p}}(a)}{e}\log_p(u(p))\,,$$

where $v_{\mathfrak{p}}$ denotes the normalized valuation of K and, for $y \in U^{(1)}$, the function is defined by the series in the statement. It is easy to check that this function is actually a continuous homomorphism and that it meets the required properties. □

Lemma 2.3.6. Let K be a p-adic number field. Let $\mathfrak{p}$ be its maximal ideal, let $v_{\mathfrak{p}}$ be its normalized valuation, and let e be the ramification index of $K/\mathbb{Q}_p$. Then, the series

$$\exp_p(x) = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots$$

converges if and only if $v_{\mathfrak{p}}(x) > \frac{e}{p-1}$. The function which it defines in the convergence region is called *p-adic exponential*.

Proof. As we already commented, since K is a non-archimedian complete field, a series $\sum_{n\geqslant 0} a_n$ converges if and only if $\lim_n a_n = 0$. A straightforward calculation shows that, if $n = \sum_{i=0}^{r} a_i p^i$, with $0 \leqslant a_i < p$, then

$$v_p(n!) = \frac{1}{p-1}\sum_{i=0}^{r} a_i(p^i - 1) = \frac{n}{p-1} - \frac{\sum_{i=0}^{r} a_i}{p-1}\,,$$

where v_p denotes the normalized valuation of $\mathbb{Q}_p$. Then,

$$v_{\mathfrak{p}}\left(\frac{x^n}{n!}\right) = n\left(v_{\mathfrak{p}}(x) - \frac{e}{p-1}\right) + e\frac{\sum_{i=0}^{r} a_i}{p-1}\,.$$

Clearly, in order that this sequence have limit zero, it is necessary that

$$v_{\mathfrak{p}}(x) - \frac{e}{p-1}\,.$$

It is also sufficient, since

$$\frac{\sum_{i=0}^{r} a_i}{p-1} \leqslant \frac{r+1}{p-1} \leqslant \frac{\log n + 1}{p-1}\,.$$

□

Lemma 2.3.7. Let K be a p-adic number field. Let $\mathfrak{p}$ be its maximal ideal, and let $U^{(n)} = 1+\mathfrak{p}^n$, for $n \in \mathbb{Z}$. Let e be the ramification index of the extension $K/\mathbb{Q}_p$. Then, for $n > e/(p-1)$, the p-adic logarithm and p-adic exponential provide continuous homomorphisms

$$\log_p : U^{(n)} \to \mathfrak{p}^n \qquad \exp_p : \mathfrak{p}^n \to U^{(n)}$$

which are inverses of each other.

Proof. Both functions are clearly continuous on the coresponding domains, since they are defined as the limit of a sequence of uniformly convergent functions. The exponential function defines a homomorphism since

$$\exp(x+y) = \exp_p(x)\exp_p(y)$$

when we consider both sides as formal power series in x and y and we have absolute convergence.

Take an integer $n > \frac{e}{p-1}$, and let v_p be the exponential valuation extending the normalized valuation of $\mathbb{Q}_p$. Then, for any $1 + x \in U^{(n)}$, with $x \neq 0$, and for any integer $k > 1$,

$$v_p\left(\frac{x^k}{k}\right) - v_p(x) = (k-1)v_p(x) - v_p(k) > \frac{k-1}{p-1} - v_p(k)\,.$$

If $k = sp^t$, with $(s,p) = 1$, then

$$\frac{k-1}{p-1} \geqslant \frac{p^t - 1}{p-1} = p^{t-1} + \cdots + p + 1 \geqslant t = v_p(k)\,.$$

Therefore, for all $k > 1$,

$$v_p\left(\frac{x^k}{k}\right) > v_p(x)\,,$$

which implies that $v_p(\log_p(1+x)) = v_p(x)$ and, consequently, $\log_p(1+x) \in \mathfrak{p}^n$.

In the same way, given $x \in \mathfrak{p}^n$, with $x \neq 0$, and any integer $k > 1$, with $k = \sum_{i=0}^{r} a_i p^i$, where $0 \leqslant a_i < p$,

$$v_p\left(\frac{x^k}{k!}\right) - v_p(x) = (k-1)v_p(x) + \frac{k-1}{p-1} + \frac{\sum_{i=0}^{r} a_i - 1}{p-1} > \frac{\sum_{i=0}^{r} a_i - 1}{p-1} \geqslant 0\,,$$

which shows that $\exp_p(x) \in U^{(n)}$.

Finally, the fact that this functions are inverse of each other follows from the observation that the coresponding formal series are inverse of each other, and the series are all absolutely convergent in the considered domains. □

Consider a p-adic number field K, with residue class field κ and $q = p^f = |\kappa|$. Since $U^{(n)} \subseteq U^{(m)}$ if $n \geqslant m$; since $\cap_{n\geqslant 1} U^{(n)} = \{1\}$, and since any sequence $(a_n)_n$ with $a_n \in U^{(1)}/U^{(n)}$ satisfying that, if $n > m$, then $a_n = a_m$ considered in $U^{(1)}/U^{(n)}$, gives rise to a Cauchy sequence in $U^{(1)}$ which converges to an element of $U^{(1)}$, we have that

$$U^{(1)} = \lim_{\leftarrow} U^{(1)}/U^{(n)}\,.$$

Since each $U^{(1)}/U^{(n)}$ has order $q^{n-1} = p^{f(n-1)}$, this identity allows us to define an operation

$$\begin{aligned} \mathbb{Z}_p \times U^{(1)} &\to U^{(1)} \\ (x, a) &\mapsto (1+x)^a \end{aligned}$$

which is immediately checked to be an action of $\mathbb{Z}_p$ on $U^{(1)}$ which gives the later a structure of $\mathbb{Z}_p$-module. It is also easy to see that the previous operation is continuous.

Proposition 2.3.8. Let K be a p-adic number field. Let κ be the residue class field and let $q = p^f = |\kappa|$. Then, we have an isomorphism of topological groups

$$K^\times \simeq \mathbb{Z} \oplus \mathbb{Z}/(q-1)\mathbb{Z} \oplus \mathbb{Z}/p^a\mathbb{Z} \oplus \mathbb{Z}_p^d\,,$$

where a is a non-negative integer and $d = [K : \mathbb{Q}_p]$.

Proof. Because of Proposition 2.3.4, we have

$$K^\times = \pi^{\mathbb{Z}} \times \mu_{q-1} \times U^{(1)}\,.$$

The topology in K clearly coincides with the product topology in the right. Therefore we get an isomorphism of topological groups

$$K^\times \simeq \mathbb{Z} \oplus \mathbb{Z}/(q-1)\mathbb{Z} \oplus U^{(1)}$$

In the previous discussion we showed that $U^{(1)}$ is a topological $\mathbb{Z}_p$-module. In the same way, the groups $U^{(n)}$ are all topological $\mathbb{Z}_p$-modules. The groups $\mathfrak{p}^n$ are also topological $\mathbb{Z}_p$-modules if we define the action of $\mathbb{Z}_p$ over $\mathfrak{p}^n$ as simply multiplication. If we take n sufficiently large (i.e. $n > e/(p-1)$, where e is the ramification index of $K/\mathbb{Q}_p$), the map

$$\log_p : U^{(n)} \to \mathfrak{p}^n$$

is an isomorphism of topological $\mathbb{Z}_p$-modules. We already know that this map is an isomorphism of topological groups, so it only remains to prove that both $\log_p$ and its inverse $\exp_p$ preserve the action of $\mathbb{Z}_p$. This can be checked directly for the action of the elements in $\mathbb{Z}$, and, therefore,

since $\mathbb{Z}$ is a dense subset of $\mathbb{Z}_p$, it is deduced for all $\mathbb{Z}_p$ by continuity of the action of $\mathbb{Z}_p$ on both groups and by continuity of the functions $\log_p$ and $\exp_p$.

Let A be the valuation ring of K, and let π be a local uniformizing parameter. We have just shown that there is an isomorphism (of topological $\mathbb{Z}_p$-modules) between $U^{(n)}$ and $\mathfrak{p}^n = \pi^n A$. Division by π^n is clearly an isomorphism of topological $\mathbb{Z}_p$-modules, so that we get an isomorphism $U^{(n)} \simeq A$. Since $\mathbb{Z}_p$ is a principal ideal domain, A is a free $\mathbb{Z}_p$-module of rank $d = [K : \mathbb{Q}_p]$. Since $[U^{(1)} : U^{(n)}] = q^{n-1}$ is finite, $U^{(1)}$ is a finitely-generated $\mathbb{Z}_p$-module of rank d with a finite torsion group. Since $U^{(1)}/U^{(n)}$ is a p-group, and $U^{(n)}$ is a free module (so that it does not contain any root of unity), the torsion elements in $U^{(1)}$ are roots of unity of order a power of p. Conversely, every root of unity of order a power of p is a torsion element in $U^{(1)}$. To prove it, let μ_{p^a} be the subgroup of roots of unity in K of order a power of p, and let ζ be a primitive p^a-root of unity. Then,

$$X^{p^{a-1}(p-1)} + \cdots + X^{p^{a-1}} + 1 = \prod_{i=1,\,(i,p)=1}^{p^a-1} \left(X - \zeta^i\right) ,$$

and, evaluating at $X = 1$,

$$p = \prod_{i=1,\,(i,p)=1}^{p^a-1} \left(1 - \zeta^i\right) .$$

It is easy to see that the elements $1 - \zeta^i$ with $(i, p) = 1$ are all related by units, so that the previous equation shows that they all are non-units. Since, for every i, $1 - \zeta^i$ is a multiple of $1 - \zeta$ (in A), this shows that all p^a-th roots of unity are in $U^{(1)}$. Since $\mathbb{Z}_p$ is a principal ideal domain, there is a free finitely-generated $\mathbb{Z}_p$ submodule V of $U^{(1)}$ such that

$$U^{(1)} = \mu_{p^a} \times V .$$

Since V is a finitely generated $\mathbb{Z}_p$-submodule, it is closed, and, since it has finite index in $U^{(1)}$, it is also open. Therefore, it is easily seen that the topology of $U^{(1)}$ coincides with the product topology in $\mu_{p^a} \times V$. We have an isomorphism of $\mathbb{Z}_p$-modules

$$U^{(1)} = \mu_{p^a} \times V \simeq \mathbb{Z}/p^a\mathbb{Z} \times \mathbb{Z}_p^d .$$

Going right-to-left is easily seen to be continue, and, since the right-hand group is compact, the previous isomorphism is also a homeomorphism.

Altogether, we get

$$K^\times \simeq \mathbb{Z} \oplus \mathbb{Z}/(q-1)\mathbb{Z} \oplus \mathbb{Z}/p^a\mathbb{Z} \oplus \mathbb{Z}_p^d .$$

□

Lemma 2.3.9. Let K be a local field of characteristic zero. Let $\mu_n(K)$ be the set of n-th roots of unity in K. Let $|\cdot|'$ denote a normalized valuation in K, i.e $|\cdot|' = |\cdot|_\infty$ if $K \simeq \mathbb{R}$, $|\cdot|' = |\cdot|_\infty^2$ if $K \simeq \mathbb{C}$ and, if K is a discrete non-archimedian field with valuation ring A, maximal ideal $\mathfrak{p}$ and residue class field κ,

$$|x|' = |\kappa|^{-\mathrm{ord}_\mathfrak{p}(x)} = |A/Ax|^{-1} .$$

Then,

$$[K^\times : K^{\times n}] = n\frac{|\mu_n(K)|}{|n|'} .$$

Proof. In the archimedian case, i.e for $K \simeq \mathbb{R}$ and $K \simeq \mathbb{C}$, the lemma follows easily.

In the non-archimedian case, K is a discrete valued field and so we have $K^\times \simeq U \times \mathbb{Z}$, where U stands for the group of units. Therefore,

$$K^{\times n} \simeq U^n \times n\mathbb{Z}$$

and

$$K^\times / K^{\times n} \simeq U/U^n \times \mathbb{Z}/n\mathbb{Z}\,,$$

from which we get

$$[K^\times : K^{\times n}] = n[U : U^n]\,.$$

By the previous proposition, and with the same notations, we know that

$$U \simeq \mu_{p^a}(K) \times \mu_{q-1} \times \mathbb{Z}_p^d \simeq \mu(K) \times \mathbb{Z}_p^d\,.$$

Consider the exact sequence

$$1 \longrightarrow \mu_n(K) \longrightarrow \mu(K) \xrightarrow{x \mapsto x^n} \mu(K) \longrightarrow \mu(K)/\mu(K)^n \longrightarrow 1$$

Using the well-known formula for the alternated product of group orders in an exact sequence, we get

$$|\mu(K)/\mu(K)^n| = |\mu_n(K)|\ .$$

On the other hand, we have

$$|\mathbb{Z}_p/n\mathbb{Z}_p|^d = \left|\mathbb{Z}/p^{v_p(n)}\mathbb{Z}_p\right|^d = p^{dv_p(n)} = \frac{1}{|n|'}\,.$$

Therefore,

$$[U : U^n] = \frac{|\mu_n(K)|}{|n|'}\,.$$

Altogether, we get, for a non-archimedian local field

$$[K^\times : K^{\times n}] = n[U : U^n] = n\frac{|\mu_n(K)|}{|n|'}\,.$$

□

2.4 Ramification of local fields

References: [Mil17a], [Neu99]

In this section K will be a non-archimedian local field, A its valuation ring, $\mathfrak{p}$ its maximal ideal, π a local uniformizing parameter and κ its residue class field. All extensions are taken within the same algebraic closure K^{al}.

Let L/K be an algebraic extension of K with ramification index e and inertia degree f. We say that the extension L/K is *unramified* if $e = 1$; otherwise, we say that it is *ramified*. If L is finite, this is obviously equivalent to the fact that $f = [\lambda : \kappa] = [L : K]$, where λ is the residue class field of L; if L is infinite, then the condition $e = 1$ is equivalent to the fact that all finite subextensions be unramified.

Proposition 2.4.1. Let L/K be an unramified extension. Then L/K is separable.

Proof. Let B be the valuation ring of L and let λ be its residue class field. Take any $\alpha \in L$ and let $f(X)$ be its minimal polynomial over K. By multiplying α by a suitable element in $K^\times$, we can assume that $\alpha \in B$ and consequently $f(X) \in A[X]$ (recall that, by the proof of Proposition 2.2.12, α is integral over A). Let $\overline{\alpha}$ be the image of α in λ. Since the subextension $K(\alpha)/K$ is unramified,

$$[K(\alpha) : K] = [\kappa(\overline{\alpha}) : K]\,,$$

so that the image of $f(X)$ in $\kappa[X]$, which we denote by $\overline{f}(X)$, must be the minimal polynomial of $\overline{\alpha}$ over κ. But, since κ is finite, this means that $\overline{f}(X)$ must be separable, and, consequently, so must be $f(X)$. □

Proposition 2.4.2. Let L/K and K'/K be finite extensions and let $L' = LK'$. Then, if L/K is unramified, so is L'/K'.

Proof. Let B be the valuation ring of L and let λ be its residue class field. Since K is a local field, the field κ is finite and hence the extension λ/κ is separable, so that there exists some $\overline{\alpha} \in \lambda$ such that $\lambda = \kappa(\overline{\alpha})$. Let $\alpha \in B$ be a lifting of $\overline{\alpha}$, let $f(X) \in A[X]$ be its minimal polynomial over K and let $\overline{f}(X)$ be its image in $\kappa[X]$. Then

$$[\lambda : \kappa] \leqslant \deg(\overline{f}) = \deg(f) = [K(\alpha) : K] \leqslant [L : K] = [\lambda : \kappa]\,,$$

so that $L = K(\alpha)$ and $\overline{f}(X)$ is the minimal polynomial of $\overline{\alpha}$ over κ.

Hence, we have $L' = K'(\alpha)$. Let A' be the valuation ring of K' and let κ' be its residue class field. Let $g(X) \in A'[X]$ be the minimal polynomial of α over K', and let $\overline{g}(X)$ be its image in $\kappa'[X]$. Then $\overline{g}(X)$ is a factor of $\overline{f}(X)$, which is separable because it is the minimal polynomial of $\overline{\alpha}$ over the finite field κ', and therefore is itself separable. This implies that $\overline{g}(X)$ is irreducible over κ', as otherwise Hensel's lemma would provide a factorization for $g(X)$. Thus, denoting by λ' the residue field of L',

$$[\lambda' : \kappa'] = \deg(\overline{g}) = \deg(g) = [L : K]\,,$$

which proves that L'/K' is unramified. □

Corollary 2.4.3. The composite of two unramified extensions of K is again unramified.

Proof. It suffices to prove the result for two finite unramified extensions, for, if the product of two (not necessarily finite) extensions is not unramified, it contains a finite ramified subextension. If L/K and L'/K are finite unramified extensions, then the previous proposition implies that LL'/L' is unramified, and therefore so is LL'/K, because the inertia degrees (and the ramification indexes) are clearly multiplicative. □

The last corollary allows to define the *maximal unramified extension* of K contained in a certain algebraic extension L as the product of all finite unramified subextensions. We will use the notation K^{un} for the maximal unramified extension contained in a certain algebraic closure.

Proposition 2.4.4. Let L be an algebraic extension of K with residue field λ. Then the map $K' \mapsto \kappa'$ sending a finite unramified extension of K contained in L to its residue field is a bijection between the set of finite unramified extensions of K contained in L and finite extensions of κ contained in λ. Moreover, this bijection preserves the order given by inclusion.

Proof. We first prove surjectivity. Let κ' be a finite extension of κ contained in λ. Since κ is finite, there exists some $\overline{\alpha} \in \kappa' \subseteq \lambda$ such that $\kappa' = \kappa(\overline{\alpha})$. Let $\overline{f}(X)$ be the minimal polynomial of $\overline{\alpha}$ over κ. Since the extension κ'/κ is separable, we have that $\overline{\alpha}$ is a simple root of $\overline{f}(X)$, so that, by Hensel's lemma, there exists a lifting α of the element $\overline{\alpha}$ to the valuation ring of L. Then clearly $K' = K(\alpha) \subseteq L$ maps to κ'.

Now, let K' and K'' be two finite unramified extensions contained in L mapping to κ'. Since, by the previous corollary, the composite $K'K''$ is also unramified, this means that

$$[K'K'' : K] = [\kappa' : \kappa] = [K' : K]$$

and, consequently, that $K = K'$.

That the given map preserves inclusions is obvious. □

Corollary 2.4.5. The maximal unramified extension K^{un} is obtained by adjoining all roots of unity of order relatively prime to the characteristic of K.

Proof. All finite extensions of a finite field can be obtained by adjoining roots of unity of order relatively prime to the characteristic. For instance, for a finite field of q elements, the (unique) extension of degree n is obtained by adjoining a root of unity of order $q^n - 1$. Therefore, since κ is a finite field, by the previous proposition we see that all finite unramified extensions can be obtained by adjoining roots of unity of order relatively prime to the characteristic, and the result follows. □

Proposition 2.4.6. Let L/K be an unramified extension and let λ be the residue class field of L. Then the extension L/K is Galois and

$$\mathrm{Gal}(L/K) \simeq \mathrm{Gal}(\lambda/\kappa)\,.$$

Proof. Let B be the valuation ring of L. Take any $\alpha \in L$, and let us prove that L contains all its conjugates over K. By multiplying α by a suitable element in $K^\times$, we may assume that $\alpha \in B$. Let $f(X) \in A[X]$ be the minimal polynomial of α over K and let $\overline{f}(X)$ be its image in $\kappa[X]$. Since λ/κ is a Galois extension (because κ is finite) the polynomial $\overline{f}(X)$ splits completely in a product of different linear factors. Therefore, by Hensel's lemma, so does $f(X)$.

Since K is complete, there is a unique extension of its valuation to L, so that every element $\sigma \in \mathrm{Gal}(L/K)$ preserves this valuation. In particular, every $\sigma \in \mathrm{Gal}(L/K)$ preserves the valuation ring and the maximal ideal of L, and hence induces a κ-isomorphism $\tilde{\sigma} : \lambda \to \lambda$. Assume that L/K is finite. By Proposition 2.4.1 the extension L/K is separable and therefore there exists some $\alpha \in L$ such that $L = K(\alpha)$. We may assume that $\alpha \in B$. Define $f = [\lambda : \kappa] = [L : K]$, and let $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_f$ be the conjugates of α. Since $[\lambda : \kappa] = [L : K]$, the minimal polynomial of α maps in $\kappa[X]$ to the minimal polynomial of the image of α in λ, whereby we deduce that the conjugates of α are distinct modulo the maximal ideal of L. Therefore, the homomorphism

$$\begin{aligned} \mathrm{Gal}(L/K) &\to \mathrm{Gal}(\lambda/\kappa) \\ \sigma &\mapsto \tilde{\sigma} \end{aligned}$$

is injective and hence an isomorphism.

If L/K is infinite, we need only take projective limits. □

We say that an extension L/K is *totally ramified* if the inertia degree of the extension is 1. This means that, for such an extension, the residue class fields of K and L are isomorphic.

Proposition 2.4.7. Let L/K be a finite totally ramified extension. Let B be the valuation ring of L and let Π be a local uniformizing parameter. Then $B = A[\Pi]$.

Proof. This follows from the proof of Proposition 2.2.14. □

Now let L/K be a finite Galois extension with Galois group $G = \mathrm{Gal}(L/K)$. Let B be the valuation ring of L, let Π be a local uniformizing parameter and let λ be its residue field. We will use the notation $|\cdot|$ for the valuation of L. For $i \geqslant 0$, define

$$G_i = \{\sigma \in G : |\sigma\alpha - \alpha| < |\Pi|^i \text{ for all } \alpha \in B\}.$$

Remark 16. Clearly $G_{i+1} \subseteq G_i$ for all $i \geqslant 0$, and $G_i = \{1\}$ for i large enough, since, for each $\sigma \in G$ with $\sigma \neq 1$, there exists some $\alpha \in B$ such that $\sigma\alpha \neq \alpha$ and $\sigma \notin G_i$ if $|\Pi|^i \leqslant |\sigma\alpha - \alpha|$.

Lemma 2.4.8. With the previous definitions and assumptions, the groups G_i are normal subgroups of G.

Proof. Let $\sigma \in G_i$. Then, for all $\tau \in G$ and for all $\alpha \in B$,

$$|\tau^{-1}\sigma\tau\alpha - \alpha| = |\tau^{-1}(\sigma\tau\alpha - \tau\alpha)| = |\sigma(\tau\alpha) - (\tau\alpha)| < |\Pi|^i.$$

□

Proposition 2.4.9. With the previous definitions and assumptions, the fixed field K_0 of G_0 is the maximal unramified extension of K contained in L.

Proof. Let K' be the maximal unramified extension of K contained in L. Then, by Proposition 2.4.4, the residue class field of K' is λ, and, by Proposition 2.4.6, the map $\sigma \mapsto \tilde{\sigma}$ provides an isomorphism $\mathrm{Gal}(K'/K) \simeq \mathrm{Gal}(\lambda/\kappa)$. Therefore, the elements $\sigma \in G$ in the kernel of the homomorphism $G \to \mathrm{Gal}(\lambda/\kappa)$ given by $\sigma \mapsto \tilde{\sigma}$ are precisely those fixing K'. But the kernel of this homomorphism is comprised of those $\sigma \in G$ such that $\sigma\alpha - \alpha \in (\Pi)$, which is precisely G_0. Consequently $K' = K_0$. □

Proposition 2.4.10. With the previous definitions and assumptions, for $i \geqslant 1$

$$G_i = \{\sigma \in G_0 : |\sigma\Pi - \Pi| < |\Pi|^i\}.$$

Proof. Obviously, any $\sigma \in G_i$ satisfies that $\sigma \in G_0$ and $|\sigma\Pi - \Pi| < |\Pi|^i$. Let A_0 be the valuation ring of K_0. Then, since L/K_0 is totally ramified, by Proposition 2.4.7 we have $B = A_0[\Pi]$, and we deduce that any $\sigma \in G_0$ satisfying that $|\sigma\Pi - \Pi| < |\Pi|^i$ lies in G_i. □

Corollary 2.4.11. The group G is solvable and an Abelian normal series is given by

$$G \triangleright G_0 \triangleright G_1 \triangleright \cdots \triangleright \{1\}.$$

Proof. The group G_0 is the kernel of the surjective homomorphism $\mathrm{Gal}(L/K) \to \mathrm{Gal}(\lambda/\kappa)$ defined by $\sigma \mapsto \tilde{\sigma}$ (see the proof of Proposition 2.4.9), so we have $G/G_0 \simeq \mathrm{Gal}(\lambda/\kappa)$, which is an Abelian group because κ is finite.

For each $\sigma \in G_0$, since it preserves the valuation, we have $\sigma\Pi = u_\sigma\Pi$ for some $u_\sigma \in B^\times$; the map $G_0 \to \lambda^\times$ defined by $\sigma \mapsto \overline{u_\sigma}$ is a homomorphism with kernel G_1, so that we get an injective homomorphism $G_0/G_1 \hookrightarrow \lambda^\times$ which shows that G_0/G_1 is Abelian.

For $i \geqslant 1$, for each $\sigma \in G_i$ we have $|\sigma\Pi - \Pi| \leqslant |\Pi|^{i+1}$, so that $\sigma\Pi = \Pi + a_\sigma\Pi^{i+1}$ for some $a_\sigma \in B$; the map $G_i \to \lambda$ defined by $\sigma \mapsto \overline{a_\sigma}$ is a homomorphism with kernel G_{i+1} and therefore we get an injective homomorphism $G_i/G_{i+1} \hookrightarrow \lambda$ which shows that G_i/G_{i+1} is Abelian. □

2.5 Extension of valuations

References: [Neu99]

Now, we will focus on the extension of a valuation to an algebraic extension in the general case (we have already seen the case when the initial field is complete). From now on, we will use the notation v to denote any kind of valuation, either a multiplicative or an exponential valuation.

Let K be a field and v a valuation on K. Let K_v denote the completion of K with respect to v, and let $\overline{K_v}$ be its algebraic closure. Since K_v is complete, we already know that there is a unique extension of v to $\overline{K_v}$, which we will denote by $\overline{v}$.

Let L/K be an algebraic extension. Then, the canonical embedding of K into $\overline{K_v}$ can be lifted to an embedding

$$\tau : L \to \overline{K_v}\,.$$

The composite of this embedding with the valuation $\overline{v}$, which we will denote by $w = \overline{v} \circ \tau$, gives a valuation of L extending the given valuation v on K. From the definition of w, it is clear that τ is continuous with respect to this valuation, so that it can be lifted to L_w:

$$\tau : L_w \to \overline{K_v}\,,$$

where L_w is the completion of L with respect to w when L/K is finite and the direct limit of the completions of all finite subextensions when it is infinite. This embedding allows us to think of L_w as an algebraic extension of K_v within $\overline{K_v}$. Then, since K_v is complete, w is the unique extension of the valuation v, defined on K_v, to a valuation on L_w, and, if L_w/K_v is finite of degree n, it is given by the formula

$$|x|_w = \sqrt[n]{|\mathrm{Nm}_{L_w/K_v}(x)|}\,.$$

Observe also that, by Lemma 2.2.11, $L_w = LK_v$ (it is an easy consequence of the lemma if L/K is finite, as the lemma clearly implies that LK_v is complete, and it also holds in the infinite case by the way in which we have defined L_w in this case).

We have seen that we can extend the valuation v to L by considering $w = \overline{v} \circ \tau$ for some K-embedding τ of L into $\overline{K_v}$. The following propositions asserts that every extension of v arises in this way.

Proposition 2.5.1. Let K be a field provided with a valuation v, and let L/K be an algebraic extension. Then, with the previous notations, every extension w of v to L can be expressed in the form $w = \overline{v} \circ \tau$ for some K-embedding τ of L into $\overline{K_v}$. Moreover, two such extensions $w = \overline{v} \circ \tau$ and $w' = \overline{v} \circ \tau'$ are equivalent if and only if $\tau' = \sigma \circ \tau$ for some $\sigma \in \mathrm{Gal}(\overline{K_v}/K_v)$.

Proof. For the first part of the proposition, let w be a valuation of L extending v. Any K_v-embedding τ of L_w in $\overline{K_v}$ gives an extension $\overline{v} \circ \tau$ of v from K_v to L_w. Since K_v is complete, there is only one valuation in L_w extending v, so that $w = \overline{v} \circ \tau$.

Now, let $w = \overline{v} \circ \tau$ and $w' = \overline{v} \circ \tau'$, where τ and τ' are K-embeddings of L into $\overline{K_v}$. Assume that $\tau' = \sigma \circ \tau$ for some $\sigma \in \mathrm{Gal}(\overline{K_v}/K_v)$. Since $\overline{v}$ is the unique valuation of $\overline{K_v}$ extending v, we have $\overline{v} \circ \sigma = \overline{v}$. Therefore,

$$w' = \overline{v} \circ \tau' = \overline{v} \circ \sigma \circ \tau = \overline{v} \circ \tau = w\,.$$

Conversely, assume that $w = w'$. Define $\sigma : \tau L \to \tau' L$ as the K-isomorphism $\sigma = \tau' \circ \tau^{-1}$. Observe that σ is a K-isomorphism between the valued fields $(\tau L, \overline{v}|_{\tau L})$ and $(\tau' L, \overline{v}|_{\tau' L})$ that

preserves the valuation, and therefore extends to a K_v-isomorphism

$$\sigma : \tau L \cdot K_v \to \tau' L \cdot K_v$$

which, in turn, can be extended to an automorphism $\sigma \in \mathrm{Gal}(\overline{K_v}/K_v)$. □

Remark 17. Because of Lemma 2.1.6 and the fact that all extensions of v must agree on K, two extensions w and w' of v to L are either equal or inequivalent.

Remark 18. As a consequence of the previous proposition, for a simple extension $L = K(\alpha)$, the extensions of the valuation correspond one to one to the different irreducible factors of the minimal polynomial of α over K when decomposed over K_v. To see it, let $f(X)$ be the minimal polynomial of α over K, and let

$$f(X) = f_1(X)^{m_1} \dots f_r(X)^{m_r}$$

be its factorization in $K_v[X]$. Any K-embedding of L into $\overline{K_v}$ must send α to a root of one of the factors $f_i(X)$, and two such embeddings are conjugate over K_v if and only if they send α to roots of the same irreducible factor.

Consider a finite extension L/K. For any valuation w of L extending v, there are natural K-embeddings of K_v and L into L_w, which allow to define a map

$$\begin{aligned} \varphi : L \otimes_K K_v &\to \prod_{w|v} L_w \\ a \otimes_K b &\mapsto (ab)_w \,. \end{aligned}$$

Both $L \otimes_K K_v$ and $\prod_{w|v} L_w$ can be regarded as K_v-algebras and it is easy to check that φ is a homomorphism of K_v-algebras.

Proposition 2.5.2. If L/K is a finite separable extension, the previous homomorphism φ is an isomorphism (of K_v-algebras).

Proof. Since L/K is finite and separable, it is simple, i.e. $L = K(\alpha)$ for some α. Let $f(X) \in K[X]$ be the minimal polynomial of α. We know that there is a one-to-one correspondence between the valuations $w|v$ and the irreducible factors $f_w(X)$ of $f(X)$ in $K_v[X]$, and, since L/K is separable,

$$f(X) = \prod_{w|v} f_w(X) \,.$$

For each $w|v$, let α_w be a root of $f_w(X)$ in $\overline{K_v}$. Then, $L_w \simeq K_v(\alpha_w)$, as $K_v(\alpha_w)$ is complete because of Lemma 2.2.11 and L can be seen as a subfield of it by the natural K-embedding sending α to α_w, which preserves valuations because of the way in which w is defined. Therefore, we find the following chain of isomorphims:

$$L \otimes_K K_v \simeq K_v[X]/(f(X)) \simeq \prod_{w|v} K_v[X]/(f_w(X)) \simeq \prod_{w|v} L_w$$

(the second isomorphism is given by the Chinese remainder theorem). The map φ is the composite of these isomorphisms. □

Corollary 2.5.3. Under the same assumtions,

$$[L : K] = \sum_{w|v} [L_w : K_v] \,,$$

and, for any $\alpha \in L$,

$$\mathrm{Nm}_{L/K}(\alpha) = \prod_{w|v} \mathrm{Nm}_{L_w/K_v}(\alpha), \quad \mathrm{Tr}_{L/K}(\alpha) = \prod_{w|v} \mathrm{Tr}_{L_w/K_v}(\alpha)\,.$$

Proof. We know that φ is an isomorphism of K_v-algebras and, in particular, of K_v-vector spaces. Then,

$$\dim_K(L) = \dim_{K_v}(L \otimes_K K_v) = \dim_{K_v}\left(\prod_{w|v} L_w\right) = \sum_{w|v} \dim_{K_v}(L_w)\,,$$

which implies the first identity.

Now, consider the homomorphism multiplication by α in L and in $L \otimes_K K_v$. Its characteristic polynomial is the same in both cases (any K-basis of L is also, with the corresponding identifications, a basis of $L \otimes_K K_v$, and, using these basis, the homomorphism multiplication by α has the same associated matrix in both L and $L \otimes_K K_v$). By the isomorphism φ, this characteristic polynomial is also the same as in $\prod_{w|v} L_w$, which in turn is the product of the characteristic polynomials of the homomorphism multiplication by α on each L_w. Altogether:

$$\mathrm{char}_{L/K,\alpha}(X) = \prod_{w|v} \mathrm{char}_{L_w/K_v,\alpha}(X)\,,$$

which implies the desired identities. □

Proposition 2.5.4. (Fundamental identity of valuation theory) For a finite separable extension L/K and a discrete non-archimedian valuation v, we have

$$\sum_{w|v} e_w f_w = [L : K]\,.$$

Proof. If L/K is a finite separable extension, so are the extensions L_w/K_v, because $L_w = K_v(L)$. Therefore, the identity follows from the previous proposition and Proposition 2.2.14. □

Now, assume that L/K is a Galois extension and let $G = \mathrm{Gal}(L/K)$. Let v be a valuation on K. Then, G acts on the set of valuations $w|v$ of L according to the rule:

$$(\sigma, w) \to \sigma w = w \circ \sigma^{-1}\,.$$

Moreover, as we see in the following proposition, this action is transitive.

Proposition 2.5.5. G acts transitively on the set of valuations $w|v$.

Proof. If v is the trivial valuation, so are all the extensions, and the statement follows trivially, so we will assume that v is not trivial.

Assume first that the extension L/K is finite, and suppose that w and w' are two extensions of v lying on different orbits of the action of G. Then, their orbits, which are comprised of the valuations of the form $|x| = |\sigma^{-1}x|_w$ and $|x| = |\sigma^{-1}x|_{w'}$, respectively, are disjoint, so that, by the weak approximation theorem, we can find $x \in L$ such that

$$|\sigma^{-1}x|_w < 1 \text{ and } |\sigma^{-1}x|_{w'} > 1 \text{ for all } \sigma \in G\,.$$

However, this implies

$$1 > \prod_{\sigma\in G} |\sigma^{-1}x|_w = |\mathrm{Nm}_{L/K}(x)|_w = |\mathrm{Nm}_{L/K}(x)|_v = |\mathrm{Nm}_{L/K}(x)|_{w'} = \prod_{\sigma\in G} |\sigma^{-1}x|_{w'} > 1\,,$$

which is a contradiction.

If L/K is infinite, let w and w' be two extensions of v and define, for each finite subextension M/K,

$$X_M = \{\sigma \in G : \sigma w|_M = w'|_M\}\,.$$

These sets are non-empty because of the finite case of the proposition. They are also closed, since, for any $\sigma \notin X_M$, the open subset $\sigma\mathrm{Gal}(L/M)$ is disjoint with X_M. Then, we claim that $\cap_M X_M$, where M runs over all finite subextensions, is non-empty. To see it, assume it is empty. Then, since G is compact, there are finite subextensions $M_1, M_2, \ldots, M_r$ such that $\cap_{i=1}^r X_{M_i}$ is empty. But, taking $M = M_1M_2\ldots M_r$, which is also a finite subextension, we have $\cap_{i=1}^r X_{M_i} = X_M$, which is non-empty and so yields a contradiction. □

Definition 2.5.6. Let $w|v$ be an extension of v to the Galois extension L/K. Then, its *decomposition group* is

$$G_w = \{\sigma \in G : \sigma w = w\}\,.$$

Lemma 2.5.7. Let $w|v$ be an extension of v to the Galois extension L/K. Then, G_w is a closed subgroup of G.

Proof. G_w is clearly a subgroup. To prove closeness, let $\sigma \in G$ be in the closure of G_w. Then, for every open neighborhood $\sigma\mathrm{Gal}(L/M)$ of σ (here M denotes a finite subextension), there exists some $\sigma_M \in \sigma\mathrm{Gal}(L/M) \cap G_w$. Since $\sigma_M \in \sigma\mathrm{Gal}(L/M)$, $\sigma|_M = \sigma_M|_M$, so that

$$w \circ \sigma|_M = w \circ \sigma_M|_M = w|_M\,.$$

As this holds for every finite subextension M, we see that $\sigma \in G_w$. □

Lemma 2.5.8. With the previous definitions, G_w consists of those $\sigma \in G$ which are continuous with respect to w.

Proof. Clearly, all $\sigma \in G_w$ is continuous with respect to w. If v is the trivial valuation, then the unique extension of v to L is w, so that $G_w = G$ and the result follows. So assume that v is not the trivial valuation (and hence neither is w). If $\sigma \in G$ is continuous with respect to w, then for all $x \in L$

$$|x|_w < 1 \Longrightarrow |x|_{\sigma^{-1}w} = |\sigma x|_w < 1\,,$$

because $|x|_w < 1$ is equivalent to the fact that the sequence $(a_n)_n$ defined by $a_n = x^n$ tends to zero with the topology defined by w. Therefore, by Lemma 2.1.6, $w = \sigma^{-1}w$ and $\sigma w = w$. □

Proposition 2.5.9. Let $w|v$ be an extension of v to the Galois extension L/K. Then, with the notations used so far,

$$G_w \simeq \mathrm{Gal}(L_w/K_v)\,.$$

Proof. Obviously, any $\sigma \in \mathrm{Gal}(L_w/K_v)$ gives, by restriction, an element $\tilde{\sigma} \in G$. Since K_v is complete, w is the unique extension of v from K_v to L_w, so that $w \circ \sigma = w$ and, consequently, $\tilde{\sigma} \in G_w$. To prove bijectivity, we need to show that any $\tau \in G_w$ can be uniquely lifted to an element $\tilde{\tau} \in \mathrm{Gal}(L_w/K_v)$, which follows from the fact that any $\tau \in G_w$ preserves the valuation w, so that it can be uniquely lifted to a map $\tilde{\tau} : L_w \to L_w$ which obviously fixes K_v. □

2.6 Valuations in number fields

References: [Neu99]

Now, we are going to particularize some of the previous results to the case of number fields.

Definition 2.6.1. A *prime* (or *place*) of a number field K is a class of equivalent valuations.

The primes corresponding to archimedian valuations are called *infinite primes*. Since a valuation of K gives, by restriction, a valuation of $\mathbb{Q}$, the infinite primes of a number field correspond to the extensions of the unique archimedian valuation $|\cdot|_\infty$ of $\mathbb{Q}$. Consequently, by Proposition 2.5.1, these primes are represented by valuations of the form $|x| = |\tau x|_\infty$ where now $|\cdot|_\infty$ represents the classical absolute value of $\mathbb{C}$ and τ is a $\mathbb{Q}$-embedding of K into $\mathbb{C}$. Also by Proposition 2.5.1, two embeddings τ and τ' give the same valuation if and only if they are conjugate. If $\tau(K) \subseteq \mathbb{R}$, we say that the corresponding prime is called a *real prime*. Otherwise, it is called a *complex prime*. Among the $[K:\mathbb{Q}]$ $\mathbb{Q}$-embeddings of K into $\mathbb{C}$, we get a real prime from each real embedding and a complex prime from each pair of conjugate complex embeddings.

The primes corresponding to non-archimedian valuations are called *finite primes*, and they must extend non-archimedian valuations of $\mathbb{Q}$, which are, up to equivalence, the p-adic valuations. If

$$(p) = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_r^{e_r} ,$$

then, for each $\mathfrak{P}_i$, the exponential valuation

$$\frac{1}{e_i}\mathrm{ord}_{\mathfrak{P}_i} ,$$

where $\mathrm{ord}_{\mathfrak{P}}(a)$ is defined as the exponent of $\mathfrak{P}$ in the factorization of the fractional ideal (a) into prime ideals, clearly extends ord_p to K. Moreover, the ramification index and inertial degree of the corresponding valuations agree with the ramification index and inertial degree defined for classical prime ideals, so that Proposition 2.5.4 implies that these are all the valuations extending ord_p.

To each prime $\mathfrak{p}$ of K, finite or infinite, we assign a normalized valuation. For an infinite prime $\mathfrak{p}|\infty$, the normalized valuation is given by:

$$|x|_{\mathfrak{p}} = |\tau x|_\infty ,$$

if $\mathfrak{p}$ is real, and by

$$|x|_{\mathfrak{p}} = |\tau x|_\infty^2 ,$$

if $\mathfrak{p}$ is complex, where in both cases τ is a $\mathbb{Q}$-embedding giving rise to the prime $\mathfrak{p}$. Actually, the definition in the case of a complex prime does not meet the definition of a valuation, as it does not satisfy the triangle inequality, but it is anyway convenient to define the normalized valuation in this way. For a finite prime $\mathfrak{p}|p$, the normalized valuation is given by:

$$|x|_{\mathfrak{p}} = \mathrm{Nm}(\mathfrak{p})^{-\mathrm{ord}_{\mathfrak{p}}(x)} = p^{-f_{\mathfrak{p}}\mathrm{ord}_{\mathfrak{p}}(x)}$$

For infinite primes, we define the residue class field as the completion $K_{\mathfrak{p}}$, so that for a extension of number fields L/K and $\mathfrak{P}|\mathfrak{p}$ the inertial degree is

$$f_{\mathfrak{P}|\mathfrak{p}} = [L_{\mathfrak{p}} : K_{\mathfrak{p}}] ,$$

which can only be 1 or 2, and the ramification index $e_{\mathfrak{P}|\mathfrak{p}}$ is always taken to be one. With these definitions, it is easy to see that Proposition 2.5.4 also holds for infinite primes.

Proposition 2.6.2. (Product formula) Let K be a number field. Then, for any $x \in K^\times$,

$$\prod_{\mathfrak{p}} |x|_{\mathfrak{p}} = 1\,,$$

where $\mathfrak{p}$ runs over all primes of K (both finite and infinite).

Proof. We begin by proving the formula in the case $K = \mathbb{Q}$. In this case, given $x \in \mathbb{Q}$,

$$\prod_{p} |x|_p = |x|_\infty \prod_{p|x} p^{-\mathrm{ord}_p(x)} = 1\,.$$

Now, let K be any number field, and take any $x \in K$. For the infinite primes we have

$$\prod_{\mathfrak{p}|\infty} |x|_{\mathfrak{p}} = \prod_{\sigma \in \mathrm{Gal}(K/\mathbb{Q})} |\sigma| = |\mathrm{Nm}_{K/\mathbb{Q}}(x)|_\infty\,.$$

For the finite primes dividing a finite prime p of $\mathbb{Q}$, we have

$$\prod_{\mathfrak{p}|p} |x|_{\mathfrak{p}} = \prod_{\mathfrak{p}|p} p^{-f_{\mathfrak{p}} \mathrm{ord}_{\mathfrak{p}}(x)} = p^{\sum_{\mathfrak{p}|p} f_{\mathfrak{p}} \mathrm{ord}_{\mathfrak{p}}(x)}\,. \tag{2.1}$$

Observe that $\frac{1}{e_{\mathfrak{p}}}\mathrm{ord}_{\mathfrak{p}}$ is the unique extension of $\mathrm{ord}_p(x)$ from $\mathbb{Q}_p$ to $K_{\mathfrak{p}}$; thus, it is given by

$$\frac{1}{e_{\mathfrak{p}}}\mathrm{ord}_{\mathfrak{p}} = \frac{1}{[K_{\mathfrak{p}} : \mathbb{Q}_p]}\mathrm{ord}_p(\mathrm{Nm}_{K_{\mathfrak{p}}/\mathbb{Q}_p}(x)) = \frac{1}{e_{\mathfrak{p}} f_{\mathfrak{p}}}\mathrm{ord}_p(\mathrm{Nm}_{K_{\mathfrak{p}}/\mathbb{Q}_p}(x))\,.$$

Therefore, we obtain

$$\sum_{\mathfrak{p}|p} f_{\mathfrak{p}}\mathrm{ord}_{\mathfrak{p}}(x) = \sum_{\mathfrak{p}|p} \mathrm{ord}_p(\mathrm{Nm}_{K_{\mathfrak{p}}/\mathbb{Q}_p}(x)) = \mathrm{ord}_p\left(\prod_{\mathfrak{p}|p} \mathrm{Nm}_{K_{\mathfrak{p}}/\mathbb{Q}_p}(x)\right) = \mathrm{ord}_p(\mathrm{Nm}_{K/\mathbb{Q}}(x))\,,$$

which, substituted in equation (2.1), gives

$$\prod_{\mathfrak{p}|p} |x|_{\mathfrak{p}} = |\mathrm{Nm}_{K_{\mathfrak{p}}/\mathbb{Q}_p}(x)|_p\,.$$

Altogether, we obtain

$$\prod_{\mathfrak{p}} |x|_{\mathfrak{p}} = \prod_{p} \prod_{\mathfrak{p}|p} |x|_{\mathfrak{p}} = \prod_{p} |\mathrm{Nm}_{K_{\mathfrak{p}}/\mathbb{Q}_p}(x)|_p = 1\,.$$

□

Chapter 3

Local class field theory

In this chapter K will always denote a non-archimedian local field and L an algebraic extension of K. All extensions will be considered within the same algebraic closure of K. We use the notation K^{s} for the separable closure of K. The groups of units of K and L are denoted by U_K and U_L; the maximal ideals by $\mathfrak{p}_K$ and $\mathfrak{p}_L$, and the residue class fields by κ and λ, respectively. The notations ord_K and ord_L will refer to the normalized exponential valuations of K and L, respectively. We also define $U_K^{(m)} = 1 + \mathfrak{p}_K^m$ and $U_L^{(m)} = 1 + \mathfrak{p}_L^m$ for all $m \geqslant 1$. Local uniformizing parameters will also be referred to as *prime elements*.

3.1 The cohomology of unramified extensions

References: [Mil13]

In this section the extension L/K will always be unramified. Set $G = \mathrm{Gal}(L/K)$.

Assume that L/K is finite. Let π be a local uniformizing parameter of K. Since L/K is unramified, π is also a local uniformizing parameter of L. Also because L/K is unramified, $G \simeq \mathrm{Gal}(\lambda/\kappa)$, where the isomorphism is the natural one. This fact allows us to regard λ and $\lambda^\times$ as G-modules. Therefore, the isomorphisms

$$\begin{aligned} U_L/U_L^{(1)} &\to \lambda^\times \\ a &\mapsto [a] \end{aligned}$$

and

$$\begin{aligned} U^{(m)}/U^{(m+1)} &\to \lambda \\ 1 + a\pi^m &\mapsto [a] \end{aligned}$$

from Proposition 2.1.10 are in fact G-isomorphisms.

Lemma 3.1.1. Assume that L/K is finite. Then $H_T^r(G, \lambda) = 0$ and $H_T^r(G, \lambda^\times) = 0$ for all $r \in \mathbb{Z}$.

Proof. Since $G \simeq \mathrm{Gal}(\lambda/\kappa)$ is cyclic, by Proposition 1.9.8 we need only prove the result for $r = 1$ and $r = 2$. In fact, since λ and $\lambda^\times$ are finite groups, by Proposition 1.9.11 the corresponding Herbrand quotients are both 1, so that it is enough to prove the result for $r = 1$. For λ this is a consequence of Proposition 1.8.6 and for $\lambda^\times$ it is a consequence of Hilbert's theorem 90 (Proposition 1.8.5). □

Remark 19. Note that, in particular, for $r = 0$, we get $\kappa/\mathrm{Tr}_{\lambda/\kappa}\lambda = H_T^0(G,\lambda) = 0$ and $\kappa^\times/\mathrm{Nm}_{\lambda/\kappa}\lambda^\times = H_T^0(G,\lambda^\times) = 0$, so that the trace map $\mathrm{Tr}_{\lambda/\kappa} : \lambda \to \kappa$ and the norm map $\mathrm{Nm}_{\lambda/\kappa} : \lambda^\times \to \kappa^\times$ are surjective.

Proposition 3.1.2. Assume that L/K is finite. Then the map $\mathrm{Nm}_{L/K} : U_L \to U_K$ is surjective.

Proof. It is straightforward that the diagram

$$\begin{array}{ccc} U_L & \longrightarrow & \lambda^\times \\ \downarrow{\scriptstyle \mathrm{Nm}_{L/K}} & & \downarrow{\scriptstyle \mathrm{Nm}_{\lambda/\kappa}} \\ U_K & \longrightarrow & \kappa^\times \end{array}$$

and the diagrams

$$\begin{array}{ccc} U_L^{(m)} & \longrightarrow & \lambda^\times \\ \downarrow{\scriptstyle \mathrm{Nm}_{L/K}} & & \downarrow{\scriptstyle \mathrm{Tr}_{\lambda/\kappa}} \\ U_K^{(m)} & \longrightarrow & \kappa^\times \end{array}$$

for $m \geqslant 1$, where the horizontal arrows are the maps from the proof of Proposition 2.1.10, are commutative. Observe that the horizontal arrows and the right vertical arrows are surjective. Therefore, given $u \in U_K$, there exists some $v_0 \in U_L$ which is mapped through the first diagram to the same element in $\kappa^\times$ as u. Therefore, we have $u/\mathrm{Nm}_{L/K}v_0 \in U_K^{(1)}$. Now, in the same way and using the corresponding diagram, we can obtain an element $v_1 \in U_L^{(1)}$ for which we have $u/\left(\mathrm{Nm}_{L/K}(v_0)\cdot\mathrm{Nm}_{L/K}(v_1)\right) = u/\mathrm{Nm}_{L/K}(v_0v_1) \in U_K^{(2)}$. Continuing in this way, we obtain a sequence $(v_n)_n$ with $v_n \in U_L^{(n)}$ such that $u/\mathrm{Nm}_{L/K}(v_0\cdots v_n) \in U_K^{(n+1)}$ for all $n \geqslant 0$. Since $v_n \in U_L^{(n)}$ for all $n \geqslant 1$, it is easy to see that the sequence $\prod_{i=0}^n v_i$ converges. Let $v = \prod_{i=0}^\infty v_i$. Since the norm map is continuous (because K is complete, so that all $\sigma \in G$ preserve the valuation of L), we have $\mathrm{Nm}_{L/K}(v) = \lim_n \mathrm{Nm}_{L/K}(v_0\cdots v_n)$, which equals u because of the property $u/\mathrm{Nm}_{L/K}(v_0\cdots v_n) \in U_K^{(n+1)}$ for all $n \geqslant 0$. □

Proposition 3.1.3. Assume that L/K is finite. Then $H_T^r(G,U_L) = 0$ for all $r \in \mathbb{Z}$.

Proof. Since G is cyclic, it suffices to prove the result for $r = 0$ and $r = 1$. For $r = 0$, it is a consequence of the previous proposition.

Now, observe that

$$L^\times = U_L \times \pi^{\mathbb{Z}}\,.$$

Since $\pi \in K$, it remains fixed by G, so that we have

$$L^\times \simeq U_L \times \mathbb{Z}$$

as G-modules, where we are considering, as usual, the trivial action on $\mathbb{Z}$. Therefore,

$$H^1(G,L^\times) \simeq H^1(G,U_L) \times H^1(G,\mathbb{Z})\,;$$

but, by Hilbert's theorem 90, $H^1(G,L^\times) = 0$, so that we have $H^1(G,U_L) = 0$. □

Corollary 3.1.4. We have $H^r(G,U_L) = 0$ for all $r > 0$ (now L/K can be infinite).

Proof. For all $r > 0$, we have

$$H^r(G, U_L) = \varinjlim H^r(G/H, U_L^H)\,,$$

where the direct limit is taken over the open subgroups H of G of finite index. This is equivalent to taking the direct limit over the finite subextensions F of L, i.e.

$$H^r(G, U_L) = \varinjlim H^r(\mathrm{Gal}(F/K), U_F)\,,$$

and the desired result follows from the finite case. □

We have just seen that $H^r(G, U_L) = 0$ for all $r > 0$. Therefore, from the short exact sequence

$$0 \longrightarrow U_L \longrightarrow L^\times \xrightarrow{\mathrm{ord}_L} \mathbb{Z} \longrightarrow 0$$

we get isomorphisms

$$H^r(G, L^\times) \xrightarrow{\simeq} H^r(G, \mathbb{Z})$$

for all $r > 0$ (and, in particular, for $r = 2$).

On the other hand, since $H^r(G, \mathbb{Q}) = 0$ for all $r > 0$ (see Lemma 1.9.7), the short exact sequence

$$0 \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Q} \longrightarrow \mathbb{Q}/\mathbb{Z} \longrightarrow 0\,,$$

gives isomorphisms

$$H^r(G, \mathbb{Q}/\mathbb{Z}) \xrightarrow{\simeq} H^{r+1}(G, \mathbb{Z})$$

for all $r > 0$ (and, in particular for $r = 1$).

For any Galois extension of fields E/F, we will write $H^2(E/F)$ for $H^2(\mathrm{Gal}(E/F), E^\times)$.

Definition 3.1.5. The *invariant map for the extension* L/K

$$\mathrm{inv}_{L/K} : H^2(L/K) \to \mathbb{Q}/\mathbb{Z}$$

is the map obtained from the composite

$$H^2(G, L^\times) \xrightarrow{\simeq} H^2(G, \mathbb{Z}) \xrightarrow{\simeq} H^1(G, \mathbb{Q}/\mathbb{Z}) \simeq \mathrm{Hom}_{\mathrm{cts}}(G, \mathbb{Q}/\mathbb{Z}) \xrightarrow{\varphi \mapsto \varphi(\mathrm{Frob}_{L/K})} \mathbb{Q}/\mathbb{Z}\,,$$

where the first two isomorphisms are the ones which we had just obtained.

Remark 20. Since the Fröbenius element $\mathrm{Frob}_{L/K}$ generates G, any $\varphi \in \mathrm{Hom}_{\mathrm{cts}}(G, \mathbb{Q}/\mathbb{Z})$ is determined by its action on $\mathrm{Frob}_{L/K}$, so that the last map in the definition of the invariant map is injective and, consequently, the invariant map is itself injective (the other arrows are isomorphisms). If L is a finite unramified extension, then, since G is cyclic, a map $\varphi \in \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z})$ can map the Fröbenius element to any element in $\frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$, so that we get an isomorphism

$$\mathrm{inv}_{L/K} : H^2(L/K) \xrightarrow{\simeq} \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}\,.$$

Lemma 3.1.6. The invariant maps are compatible in the sense that, if L and M are unramified extensions of K and $L \subseteq M$, then the diagram

$$\begin{array}{ccc} H^2(L/K) & \xrightarrow{\mathrm{inv}_{L/K}} & \mathbb{Q}/\mathbb{Z} \\ \Big\downarrow{\scriptstyle \mathrm{Inf}} & & \Big\downarrow{\scriptstyle =} \\ H^2(M/K) & \xrightarrow{\mathrm{inv}_{M/K}} & \mathbb{Q}/\mathbb{Z} \end{array}$$

is commutative.

Proof. Thinking of the cohomology groups in terms of cochains, it is straghtforward to check that the inflation map is compatible with all the homomorphisms in the definition of the invariant maps. □

Proposition 3.1.7. The map

$$\mathrm{inv}_{K^{\mathrm{un}}/K} : H^2(K^{\mathrm{un}}/K) \to \mathbb{Q}/\mathbb{Z}$$

is an isomorphism.

Proof. We have already seen that the invariant maps are injective, so that we need only prove surjectivity. To that end, observe that, by the previous lemma, for every finite unramified extension L/K we have the commutative diagram

$$\begin{array}{ccc} H^2(L/K) & \xrightarrow{\mathrm{inv}_{L/K}} & \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z} \\ \Big\downarrow{\scriptstyle \mathrm{Inf}} & & \Big\downarrow \\ H^2(K^{\mathrm{un}}/K) & \xrightarrow{\mathrm{inv}_{K^{\mathrm{un}}/K}} & \mathbb{Q}/\mathbb{Z} \end{array},$$

where the first arrow is an isomorphism. Since K is a local field, there exist finite unramified extensions of all finite degree (recall that the finite unramified extensions of K are in bijection with the finite extensions of κ, which is a finite field), whereby surjectivity follows. □

Remark 21. Since

$$H^2(K^{\mathrm{un}}/K) \simeq \varinjlim H^2(F/K)\,,$$

where the direct limit is taken over all finite subextensions of K^{un}/K and the homomorphisms defining the direct limit are precisely the inflation maps, the map $\mathrm{inv}_{K^{\mathrm{un}}/K}$ is uniquely determined by the maps $\mathrm{inv}_{F/K}$ defined for finite unramified extensions F.

Until the end of this section, we will use the simplified notation inv_K to denote the map $\mathrm{inv}_{K^{\mathrm{un}}/K}$.

Assume that L/K is finite. The element of $H^2(L/K)$ which is mapped to $\frac{1}{[L:K]} \in \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$ by the isomorphism $\mathrm{inv}_{L/K}$ will be referred to as the *local fundamental class for the extension* L/K and will be denoted by $u_{L/K}$.

The G-module $L^\times$ satisfies the hypothesis of Tate's theorem: for every subgroup H of G we have that $H^1(H, L^\times) = 0$ because of Hilbert's theorem 90, and $H^2(H, L^\times) = H^2(L/L^H)$ is cyclic of order $|H|$ because of the isomorphism

$$\mathrm{inv}_{L/L^H} : H^2(L/L^H) \to \frac{1}{[L : L^H]}\mathbb{Z}/\mathbb{Z}\,.$$

Therefore, by Tate's theorem, cup-product with the fundamental class $u_{L/K}$ provides isomorphisms

$$H_T^r(G,\mathbb{Z}) \to H_T^{r+2}(G,L^\times)$$

for all $r \in \mathbb{Z}$. In particular, for $r=-2$ and taking into account the isomorphism

$$G = G^{\mathrm{ab}} \simeq H^2(G,\mathbb{Z})$$

from Proposition 1.9.2, we get an isomorphism

$$\gamma_{L/K} : G \to K^\times/\mathrm{Nm}_{L/K}L^\times\,.$$

Lemma 3.1.8. Assume that L/K is finite. Let $\sigma = \mathrm{Frob}_{L/K}$, let π be a local uniformizing parameter of K and let $n=[L:K]$. Then, the fundamental class $u_{L/K}$ is represented by the cochain φ defined by

$$\varphi(\sigma^i,\sigma^j) = \begin{cases} 1 & \text{if } i+j \leqslant n-1 \\ \pi & \text{if } i+j > n-1 \end{cases}\quad .$$

Proof. The preimage of $\frac{1}{n} \in \frac{1}{n}\mathbb{Z}/\mathbb{Z}$ by the last map from the definition of the invariant map $\mathrm{inv}_{L/K}$ is the unique $\chi \in \mathrm{Hom}(G,\mathbb{Q}/\mathbb{Z}) \simeq H^1(G,\mathbb{Q}/\mathbb{Z})$ such that $\chi(\sigma)=\frac{1}{n}$, i.e. it is the element of $H^1(G,\mathbb{Q}/\mathbb{Z})$ represented by the 1-cochain defined by

$$\chi(\sigma^i) = \frac{i}{n}\,.$$

It is straightforward to perform the calculation of the image of this element by the connecting map

$$H^1(G,\mathbb{Q}/\mathbb{Z}) \to H^2(G,\mathbb{Z})$$

coming from the short exact sequence

$$0 \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Q} \longrightarrow \mathbb{Q}/\mathbb{Z} \longrightarrow 0\quad ,$$

which yields the 2-cochain defined by

$$\varphi(\sigma^i,\sigma^j) = \begin{cases} 0 & \text{if } i+j \leqslant n-1 \\ 1 & \text{if } i+j > n-1 \end{cases}\quad .$$

Finally, taking into account that π remains fixed by G and $\mathrm{ord}_L(\pi)=1$, we obtain the desired result. □

Proposition 3.1.9. With the previous definitions and assumptions, the map $\gamma_{L/K}$ maps the Fröbenius element σ to the class of prime elements in $K^\times\mathrm{Nm}_{L^\times}$.

Proof. From the proof of Tate's theorem (Theorem 1.9.14), the isomorphism

$$H_T^{-2}(G,\mathbb{Z}) \to H_T^0(G,L^\times)$$

is obtained as the composite of the connecting maps

$$H_T^{-2}(G,\mathbb{Z}) \to H_T^{-1}(G,I_G)$$

and

$$H_T^{-1}(G, I_G) \to H_T^0(G, L^\times)$$

coming from the short exact sequences

$$0 \longrightarrow I_G \longrightarrow \mathbb{Z}[G] \longrightarrow \mathbb{Z} \longrightarrow 0$$

and

$$0 \longrightarrow L^\times \longrightarrow L^\times(\varphi) \longrightarrow I_G \longrightarrow 0\,,$$

respectively. The isomorphism $G \simeq H^{-2}(G, \mathbb{Z})$ is obtained through de composite of the first of the previous connecting maps and the homomorphism

$$\begin{aligned} H_T^{-1}(G, I_G) = I_G/I_G^2 &\to G^{\mathrm{ab}} = G \\ g - 1 + I_G^2 &\mapsto g \end{aligned}$$

(see Proposition 1.9.2). Therefore, it is clear that the Fröbenius element σ is mapped to $\sigma - 1 + I_G^2$ in I_G/I_G^2.

The second connecting map comes from applying the snake lemma to the diagram

$$\begin{array}{ccccccc} & & L_G^\times & \longrightarrow & L^\times(\varphi)_G & \longrightarrow & (I_G)_G \longrightarrow 0 \\ & & \downarrow{\scriptstyle \mathrm{Nm}_G} & & \downarrow{\scriptstyle \mathrm{Nm}_G} & & \downarrow{\scriptstyle \mathrm{Nm}_G} \\ 0 & \longrightarrow & L^{\times G} & \longrightarrow & L^\times(\varphi)^G & \longrightarrow & I_G^G \end{array}\,,$$

as it was defined through the diagram (1.9). In particular, it is the map going from the kernel of the last vertical arrow to the cokernel of the first vertical arrow. The group $H_T^{-1}(G, I_G) = I_G/I_G^2$ coincides with $(I_G)_G$, and a preimage of $\sigma - 1 + I_G^2$ in $L^\times(\varphi)_G = L^\times(\varphi)/I_G L^\times(\varphi)$ is given by $x_\sigma + I_G L^\times(\varphi)$. For $i = 0, 1, \ldots, n-1$, we have

$$\sigma^i x_\sigma = x_{\sigma^{i+1}} - x_{\sigma^i} + \varphi(\sigma, \sigma^i)\,,$$

where $x_{\mathrm{id}} = \varphi(1, 1) = 1$. Hence,

$$\mathrm{Nm}_G x_\sigma = \prod_{i=0}^{n-1} \varphi(\sigma, \sigma^i) = \pi\,,$$

whereby the desired result follows. □

3.2 The cohomology of ramified extensions

References: [Mil13], [Ser67]

In this section L/K need no longer be unramified.

Assume that L/K is finite. Since, for a local field, the maximal unramified extension is obtained by adjoining all roots of unity of order relatively prime to the characteristic of the residual field (see Corollary 2.4.5), we have $L^{\mathrm{un}} = L \cdot K^{\mathrm{un}}$. Therefore, the map

$$\begin{aligned} \mathrm{Gal}(L^{\mathrm{un}}/L) &\to \mathrm{Gal}(K^{\mathrm{un}}/K) \\ \sigma &\mapsto \sigma|_{K^{\mathrm{un}}} \end{aligned}$$

is injective. We will use the notation Res (i.e. the same that for restriction maps) for the map obtained from the pair of compatible homomorphisms consisting of the previous homomorphism and the natural inclusion $K^{\mathrm{un}\times} \hookrightarrow L^{\mathrm{un}\times}$.

Proposition 3.2.1. With the previous definitions, the diagram

$$\begin{array}{ccc} H^2(K^{\mathrm{un}}/K) & \xrightarrow{\mathrm{inv}_K} & \mathbb{Q}/\mathbb{Z} \\ \downarrow{\scriptstyle \mathrm{Res}} & & \downarrow{\scriptstyle [L:K]} \\ H^2(L^{\mathrm{un}}/L) & \xrightarrow{\mathrm{inv}_L} & \mathbb{Q}/\mathbb{Z} \end{array}$$

commutes.

Proof. Let e and f be the ramification index and the inertia degree, respectively, of the extension L/K, and let Γ_K and Γ_L be the Galois groups of the extensions K^{un}/K and L^{un}/L, respectively. We will prove that the diagram

$$\begin{array}{ccccccc} H^2(K^{\mathrm{un}}/K) & \xrightarrow{\mathrm{ord}_K} & H^2(\Gamma_K,\mathbb{Z}) & \xrightarrow{\delta^{-1}} & H^1(\Gamma_K,\mathbb{Q}/\mathbb{Z}) & \xrightarrow{\varphi\,\mapsto\,\varphi(\mathrm{Frob}_K)} & \mathbb{Q}/\mathbb{Z} \\ \downarrow{\scriptstyle \mathrm{Res}} & & \downarrow{\scriptstyle e\mathrm{Res}} & & \downarrow{\scriptstyle e\mathrm{Res}} & & \downarrow{\scriptstyle ef\mathrm{Res}} \\ H^2(L^{\mathrm{un}}/L) & \xrightarrow{\mathrm{ord}_L} & H^2(\Gamma_L,\mathbb{Z}) & \xrightarrow{\delta^{-1}} & H^1(\Gamma_L,\mathbb{Q}/\mathbb{Z}) & \xrightarrow{\varphi\,\mapsto\,\varphi(\mathrm{Frob}_L)} & \mathbb{Q}/\mathbb{Z} \end{array}$$

commutes. The first square commutes since $\mathrm{ord}_L|_{K^{\mathrm{un}}} = e \cdot \mathrm{ord}_K$. The second square commutes because the restriction map is compatible with the connecting map. Finally, the third square commutes because $\mathrm{Frob}_L|_{K^{\mathrm{un}}} = \mathrm{Frob}_K^f$. □

For any finite extension L/K, we will use the notation $H^2(L/K)_{\mathrm{un}}$ to denote the kernel of the map

$$\mathrm{Res} : H^2(K^{\mathrm{un}}/K) \to H^2(L^{\mathrm{un}}/L)\,.$$

Lemma 3.2.2. Assume that L/K is a finite separable extension. Then, the group $H^2(L/K)$ contains a cyclic subgroup of order $[L:K]$.

Proof. Consider the diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & H^2(L/K)_{\mathrm{un}} & \longrightarrow & H^2(K^{\mathrm{un}}/K) & \xrightarrow{\mathrm{Res}} & H^2(L^{\mathrm{un}}/L) \\ & & & & \downarrow{\scriptstyle \mathrm{Inf}} & & \downarrow{\scriptstyle \mathrm{Inf}} \\ 0 & \longrightarrow & H^2(L/K) & \xrightarrow{\mathrm{Inf}} & H^2(K^{\mathrm{s}}/K) & \xrightarrow{\mathrm{Res}} & H^2(K^{\mathrm{s}}/L) \end{array}\,.$$

It is straightforward to check that it commutes by using the description of the cohomology groups in terms of cochains. The first row is clearly exact, and the second row is also exact because of Hilbert's theorem 90 (we are using Proposition 1.4.6).

Since the inflation maps appearing in the diagram are injective (again by Hilbert's theorem 90), and in particular so is the first vertical arrow, the diagram induces an injective homomorphism

$$H^2(L/K)_{\mathrm{un}} \to H^2(L/K)\,.$$

Finally, using the commutative diagram from the previous proposition, where the rows are isomorphisms, we deduce that $H^2(L/K)_{\mathrm{un}}$ is cyclic of order $[L:K]$, which completes the proof. □

We now need the following lemma on G-modules.

Lemma 3.2.3. Let M be a G-module and let $M = M_0 \supset M_1 \supset M_2 \supset \cdots$ be a decreasing sequence of G-modules such that $M = \varinjlim M/M_i$. If for some $r > 0$ it holds that $H^r(G, M_i/M_{i+1}) = 0$ for all $i \geqslant 0$, then $H^r(G, M) = 0$.

Proof. Assume that, for some $r > 0$, we have $H^r(M_i/M_{i+1}) = 0$ for all $i \geqslant 0$. Let φ be an r-cocycle in $C^r(G, M)$. Since $H^r(G, M/M_1) = 0$, there exists an $r-1$-cochain $\psi_1 \in C^{r-1}(G, M)$ and an r-cocycle $\varphi_1 \in C^r(G, M_1)$ such that $\varphi = \mathrm{d}\psi_1 + \varphi_1$. Now, since $H^r(G, M_1/M_2) = 0$, there exists an $r-1$-cochain $\psi_2 \in C^{r-1}(G, M_1)$ and an r-cocycle $\varphi_2 \in C^r(G, M_2)$ such that $\varphi_1 = \mathrm{d}\psi_2 + \varphi_2$. Continuing in this way, we find a sequence of $r-1$ cochains $\psi_i \in C^{r-1}(G, M_{i-1})$ and a sequence of r-cocycles $\varphi_i \in C^r(G, M_i)$ such that $\varphi_i = \mathrm{d}\psi_{i+1} + \varphi_{i+1}$ for all $i \geqslant 0$. Since $M = \varinjlim M/M_i$, we can define the cochain $\psi = \sum_{i=1}^{\infty} \psi_i \in C^{r-1}(G, M)$, and we easily see that $\varphi = \mathrm{d}\psi$. □

Proposition 3.2.4. Assume that L/K is a finite Galois extension with $G = \mathrm{Gal}(L/K)$. Then there exists an open subgroup V of U_L such that $H^r(G, V) = 0$ for all $r > 0$.

Proof. By the normal basis theorem, there exists some $\alpha \in L$ such that the set $\{\sigma\alpha\}_{\sigma \in G}$ is a K-basis of L. By multiplying α by some suitable $c \in \mathcal{O}_K$, we can assume that $\alpha \in \mathcal{O}_L$ (and therefore $\sigma\alpha \in \mathcal{O}_L$ for all $\sigma \in G$, since the valuation of L is invariant under G). Define $A = \sum_{\sigma \in G} \mathcal{O}_K \sigma\alpha \subseteq \mathcal{O}_L$. Since $\{\sigma\alpha\}_{\sigma \in G}$ is a K-basis of L, we know that $\mathrm{disc}(A/\mathcal{O}_K)\mathcal{O}_L \subseteq A$, whereby we deduce that A is open. Consequently, we have $\pi_K^N \mathcal{O}_L \subseteq A$ for N sufficiently large. Fix some such N. Take some $i \geqslant N+1$ and define $M = \pi_K^i A$. Then,

$$M \cdot M = \pi_K^{2i} A \cdot A \subseteq \pi_K^{2i} \mathcal{O}_L \subseteq \pi_K \pi_K^i A = \pi_K M\,.$$

Let $V = 1 + M$. It is an open subgroup of U_L. Define $V_k = 1 + \pi_K^k M$ for $k \geqslant 0$. It is straightforward to check that this sets are in fact subgroups of U_L. Moreover, they form a fundamental system of neighborhoods of 1, so that, by the previous lemma, in order to prove that $H^r(G, V) = 0$ for all $r > 0$, we need only prove that $H^r(G, V_k/V_{k+1}) = 0$ for all $r > 0$ and for all $k \geqslant 0$. The map $V_k \to M/\pi_K M$ sending any $1 + \pi_K^k \beta$ with $\beta \in M$ to the class of β in $M/\pi_K M$ is a homomorphism of G-modules with kernel V_{k+1}, so that it induces an isomorphism of G-modules $V_k/V_{k+1} \simeq M/\pi_K M$. But $M/\pi_K M \simeq A/\pi_K A \simeq \kappa[G] = \mathrm{Ind}^G \kappa$, where $\kappa = \mathcal{O}_K/\pi_K\mathcal{O}_K$, so that it has trivial cohomology for $r > 0$. □

Lemma 3.2.5. Assume that L/K is a finite cyclic extension of degree n. Then $h(G, U_L) = 1$ and $h(G, L^\times) = n$.

Proof. Let $G = \mathrm{Gal}(L/K)$. By the previous proposition, there exists an open subgroup V of U_L such that $H^r(G, V) = 0$ for all $r > 0$. Therefore, we have $h(G, V) = 1$ by Proposition 1.9.8. Since U_L is compact and V is an open subgroup, the quotient U_L/V is finite and, consequently, we also have $h(G, U_L) = 1$ (Corollary 1.9.12).

Now, observe that $L^\times/U_L \simeq \mathbb{Z}$ as G-modules, because G preserves the valuation of L. Therefore, we have

$$h(G, L^\times) = h(G, U_L) \cdot h(G, \mathbb{Z}) = \frac{|H_T^0(G, \mathbb{Z})|}{|H^1(G, \mathbb{Z})|} = n$$

(we have used Proposition 1.9.10 and Lemma 1.9.7). □

Proposition 3.2.6. Assume that L/K is a finite Galois extension. Then $H^2(L/K)$ is a cyclic group of order $[L : K]$.

Proof. We will argue by induction on n. For cyclic extensions the proposition is a direct consequence of the previous lemma. Now, let L/K be a Galois extension and assume that it is not cyclic. Since $\mathrm{Gal}(L/K)$ is solvable because of Corollary 2.4.11, there exists a non-trivial cyclic subextension K'/K of L/K. Now, from the exact sequence

$$0 \longrightarrow H^2(K'/K) \xrightarrow{\mathrm{Inf}} H^2(L/K) \xrightarrow{\mathrm{Res}} H^2(L/K')$$

and using the induction hypothesis, we deduce

$$|H^2(L/K)| \leqslant |H^2(K'/K)| \cdot |H^2(L/K')| = [L : K] .$$

Since, by Lemma 3.2.2, the group $H^2(L/K)$ contains a cyclic subgroup of order $[L : K]$, it must be itself a cyclic group of order $[L : K]$. □

Proposition 3.2.7. The inflation map

$$\mathrm{Inf} : H^2(K^{\mathrm{un}}/K) \to H^2(K^{\mathrm{s}}/K)$$

is an isomorphism.

Proof. By Hilbert's theorem 90, this map is injective, so that we need only prove surjectivity. For any finite Galois extension L, the injective homomorphism

$$H^2(L/K)_{\mathrm{un}} \to H^2(L/K)$$

from the proof of Lemma 3.2.2 is in fact an isomorphism, because we now know that both groups have order $[L : K]$. Since

$$H^2(K^{\mathrm{s}}/K) = \varinjlim H^2(L/K) ,$$

where L runs through all finite Galois extensions K, we obtain the desired result. □

Definition 3.2.8. The *invariant map of* K is the map $\mathrm{inv}_K : H^2(K^{\mathrm{s}}/K) \to \mathbb{Q}/\mathbb{Z}$ obtained from the composite

$$H^2(K^{\mathrm{s}}/K) \xrightarrow{\mathrm{Inf}^{-1}} H^2(K^{\mathrm{un}}/K) \xrightarrow{\mathrm{inv}_{K^{\mathrm{un}}/K}} \mathbb{Q}/\mathbb{Z} .$$

If L/K is a Galois extension, the *invariant map for* L/K is the map $\mathrm{inv}_{L/K}$ obtained from the composite

$$H^2(L/K) \xrightarrow{\mathrm{Inf}} H^2(K^{\mathrm{s}}/K) \xrightarrow{\mathrm{inv}_K} \mathbb{Q}/\mathbb{Z} .$$

Remark 22. It is clear that, for unramified extensions L/K, the invariant map $\mathrm{inv}_{L/K}$ which we have just defined agrees with that of Definition 3.1.5.

Remark 23. By Proposition 3.1.7, the map inv_K is an isomorphism and, for every Galois extension L/K, the map $\mathrm{inv}_{L/K}$ is injective.

Proposition 3.2.9. Assume that L/K is a finite separable extension. Then, the diagram

$$\begin{array}{ccc} H^2(K^{\mathrm{s}}/K) & \xrightarrow{\mathrm{inv}_K} & \mathbb{Q}/\mathbb{Z} \\ \big\downarrow{\scriptstyle \mathrm{Res}} & & \big\downarrow{\scriptstyle [L : K]} \\ H^2(K^{\mathrm{s}}/L) & \xrightarrow{\mathrm{inv}_L} & \mathbb{Q}/\mathbb{Z} \end{array}$$

commutes.

Proof. The result follows from the commutativity of the diagram

$$\begin{array}{ccccc} H^2(K^{\mathrm{s}}/K) & \xleftarrow[\mathrm{Inf}]{} & H^2(K^{\mathrm{un}}/K) & \xrightarrow{\mathrm{inv}_{K^{\mathrm{un}}/K}} & \mathbb{Q}/\mathbb{Z} \\ \downarrow{\scriptstyle \mathrm{Res}} & & \downarrow{\scriptstyle \mathrm{Res}} & & \downarrow{\scriptstyle [L:K]} \\ H^2(K^{\mathrm{s}}/L) & \xleftarrow[\mathrm{Inf}]{} & H^2(L^{\mathrm{un}}/L) & \xrightarrow{\mathrm{inv}_{L^{\mathrm{un}}/L}} & \mathbb{Q}/\mathbb{Z} \end{array} .$$

Commutativity of the first square is straightforward and commutativity of the second square is Proposition 3.2.1. □

For a finite separable extension L/K, not necessarily Galois, we define $H^2(L/K)$ as the kernel of the restriction map

$$\mathrm{Res} : H^2(K^{\mathrm{s}}/K) \to H^2(K^{\mathrm{s}}/L) .$$

When L/K is Galois, this definition agrees with the one we had already given. The commutative diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & H^2(L/K) & \longrightarrow & H^2(K^{\mathrm{s}}/K) & \xrightarrow{\mathrm{Res}} & H^2(K^{\mathrm{s}}/L) \\ & & & & \downarrow{\scriptstyle \mathrm{inv}_K} & & \downarrow{\scriptstyle \mathrm{inv}_L} \\ 0 & \longrightarrow & \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z} & \longrightarrow & \mathbb{Q}/\mathbb{Z} & \xrightarrow{[L:K]} & \mathbb{Q}/\mathbb{Z} \end{array}$$

has exact rows and the vertical arrows are isomorphisms, so that it provides an isomorphism

$$\mathrm{inv}_{L/K} : H^2(L/K) \to \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z} .$$

When L/K is a Galois extension this agrees with the invariant map for L/K.

For a finite Galois extension L/K, the preimage of $\frac{1}{[L:K]}$ by $\mathrm{inv}_{L/K}$ will be referred to as the *fundamental class for* L/K and will be denoted by $u_{L/K}$.

Lemma 3.2.10. Assume that L/K is a finite separable extension. Then, the diagram

$$\begin{array}{ccc} H^2(K^{\mathrm{s}}/L) & \xrightarrow{\mathrm{inv}_L} & \mathbb{Q}/\mathbb{Z} \\ \downarrow{\scriptstyle \mathrm{Cor}} & & \downarrow{\scriptstyle =} \\ H^2(K^{\mathrm{s}}/K) & \xrightarrow{\mathrm{inv}_K} & \mathbb{Q}/\mathbb{Z} \end{array}$$

commutes.

Proof. Because of Proposition 3.2.9, the map

$$\mathrm{Res} : H^2(K^{\mathrm{s}}/K) \to H^2(K^{\mathrm{s}}/L)$$

is surjective. Therefore, we need only prove that

$$\mathrm{inv}_K(\mathrm{Cor}(\mathrm{Res}(x))) = \mathrm{inv}_L(\mathrm{Res}(x))$$

for all $x \in H^2(K^{\mathrm{s}}/K)$, which follows from Proposition 3.2.9 and Proposition 1.4.3. □

Lemma 3.2.11. Assume that L/K is a finite Galois extension and let E be a subextension of L/K. Then

$$\begin{aligned}\mathrm{Res}(u_{L/K}) &= u_{L/E}\\ \mathrm{Cor}(u_{L/E}) &= [E:K]u_{L/K}\end{aligned}$$

and, if E/K is a Galois extension,

$$\mathrm{Inf}(u_{E/K}) = [L:E]u_{L/K}\,,$$

where the maps Res, Cor and Inf are the obvious ones so that the expressions make sense.

Proof. The first identity is a consequence of the commutativity of the diagram

$$\begin{array}{ccccc} H^2(L/K) & \xrightarrow{\mathrm{Inf}} & H^2(K^{\mathrm{s}}/K) & \xrightarrow{\mathrm{inv}_K} & \mathbb{Q}/\mathbb{Z} \\ \downarrow{\scriptstyle \mathrm{Res}} & & \downarrow{\scriptstyle \mathrm{Res}} & & \downarrow{\scriptstyle [E:K]} \\ H^2(L/E) & \xrightarrow{\mathrm{Inf}} & H^2(K^{\mathrm{s}}/E) & \xrightarrow{\mathrm{inv}_E} & \mathbb{Q}/\mathbb{Z} \end{array}$$

(commutativity of the first square is straightforward and commutativity of the second square is Proposition 3.2.9).

For the second indentity, we make use of the first one and the fact that the composite

$$H^2(L/K) \xrightarrow{\mathrm{Res}} H^2(L/E) \xrightarrow{\mathrm{Cor}} H^2(L/K)$$

is multiplication by $[\mathrm{Gal}(L/K):\mathrm{Gal}(L/E)] = [E:K]$:

$$\mathrm{Cor}(u_{L/E}) = \mathrm{Cor}(\mathrm{Res}(u_{L/K})) = [E:K]u_{L/K}\,.$$

Finally, if E/K is Galois,

$$\mathrm{inv}_{L/K}(\mathrm{Inf}(u_{E/K})) = \mathrm{inv}_{E/K}(u_{E/K})) = \frac{1}{[E:K]} = [L:E]\cdot \mathrm{inv}_K(u_{L/K})\,,$$

whereby we deduce the third identity. □

3.3 The local Artin map

References: [Mil13], [Ser67], [Ser79]

As in the unramified case, for any finite Galois extension L of K, the G-module $L^\times$ satisfies the hypothesis of Tate's theorem. Hence, cup product with the fundamental class defines isomorphisms

$$H_T^r(G,\mathbb{Z}) \to H_T^{r+2}(G, L^\times)$$

for all $r \in \mathbb{Z}$. In particular, for $r = -2$ we get an isomorphism

$$\gamma_{L/K} : G^{\mathrm{ab}} \simeq H_T^{-2}(G,\mathbb{Z}) \to K^\times/\mathrm{Nm}_{L/K}L^\times\,,$$

where the isomorphism $G^{\mathrm{ab}} \simeq H_T^{-2}(G,\mathbb{Z})$ is that of Proposition 1.9.2.

Definition 3.3.1. Assume that L/K is a finite Galois extension. Then, the *local Artin map for* L/K, denoted by $\phi_{L/K}$, is the inverse of $\gamma_{L/K}$:

$$\phi_{L/K} = \gamma_{L/K}^{-1} : K^\times/\mathrm{Nm}_{L/K}L^\times \to G^{\mathrm{ab}}\,.$$

Remark 24. We will use the same terminology and notation for the map

$$\phi_{L/K} : K^\times \to G^{\mathrm{ab}}$$

obtained from the inverse of $\gamma_{L/K}$ in the natural way.

We will now require three technical lemmas involving cup-products.

Lemma 3.3.2. Let G be a finite group, and let A and B be G-modules. Given an element $a \in A^G$, define $f_a : \mathbb{Z} \to A$ as the G-homomorphism sending 1 to a. We denote by $\bar{a}$ the class of a in $A^G/\mathrm{Nm}_G A = H_T^0(G, A)$. Then, for any $x \in H_T^n(G, B)$, the element

$$\bar{a} \cup x \in H_T^n(G, A \otimes B)$$

is the image of x under the homomorphism induced in cohomology by the G-homomorphism $f_a \otimes \mathrm{Id} : B \to A \otimes B$.

Proof. For $n = 0$, the result follows directly from the definition of cup-product. We use induction on n. We begin proving the result for $n > 0$. We know that there exists a split exact sequence of G-modules

$$0 \longrightarrow B \longrightarrow B' \longrightarrow B'' \longrightarrow 0$$

in which B' is an induced G-module (this was explained at the end of section 1.2). Therefore, the connecting maps

$$\delta : H_T^n(G, B'') \to H_T^{n+1}(G, B)$$

are isomorphisms. In particular, any $x \in H_T^{n+1}(G, B)$ can be written as $x = \delta y$ for some $y \in H_T^n(G, B'')$, and we have

$$\bar{a} \cup x = \bar{a} \cup \delta y = \delta(\bar{a} \cup y)\,,$$

whereby the result follows by induction for $n > 0$.

For $n < 0$, we use the split exact sequence

$$0 \longrightarrow C \longrightarrow C' \longrightarrow B \longrightarrow 0$$

obtained by tensoring the augmentation sequence with B. Again, the midterm C is induced so that the connecting maps

$$\delta : H_T^{n-1}(G, B) \to H_T^n(G, C)$$

are isomorphisms. For any $x \in H_T^{n-1}(G, B)$, we have

$$\delta(\bar{a} \cup x) = \bar{a} \cup \delta x\,,$$

and the injectivity of δ allows us to prove that $\bar{a} \cup x$ is the desired element from the induction hypothesis. □

Lemma 3.3.3. Let G be a finite group and let A and B be G-modules. Let $a \in A$ be an element such that $\mathrm{Nm}_G a = 0$, and let $\bar{a}$ denote its class in $\ker \mathrm{Nm}_G / I_G M = H_T^{-1}(G, A)$. Let $\varphi : G \to B$ be a 1-cocycle and let $\bar{\varphi}$ denote its class in $H_T^1(G, B)$. Then, the element

$$\bar{a} \cup \bar{\varphi} \in H_T^0(G, A \otimes B)$$

is the class of the element

$$c = -\sum_{g \in G} ga \otimes \varphi(g) \in (A \otimes B)^G .$$

Proof. First of all, let us check that we have $c \in (A \otimes B)^G$. For any $h \in G$, we have

$$\begin{aligned} hc &= -\sum_{g \in G} hga \otimes h\varphi(g) = -\sum_{g \in G} hga \otimes \varphi(hg) + \sum_{g \in G} hga \otimes \varphi(h) = \\ &= -\sum_{g \in G} ga \otimes \varphi(g) + \mathrm{Nm}_G a \otimes \varphi(h) = c , \end{aligned}$$

where in the second equality we have used that, since φ is a cocycle,

$$\varphi(hg) = h\varphi(g) + \varphi(h) .$$

As in the proof of the previous lemma, we make use of the split exact sequence

$$0 \longrightarrow B \longrightarrow B' \longrightarrow B'' \longrightarrow 0$$

in which B' is induced. Then, the connecting map

$$\delta : B''^G = H^0(G, B'') \to H^1(G, B)$$

is surjective. Let $b'' \in B''^G$ be a preimage of $\bar{\varphi}$ under this map, and let $\bar{b''}$ denote its class in $H_0^T(G, B'')$. Then, denoting by $\overline{a \otimes b''}$ the class of $a \otimes b''$ in $H_T^{-1}(G, A \otimes B'')$, we have

$$\bar{a} \cup \bar{\varphi} = \bar{a} \cup \delta \bar{b''} = -\delta(\bar{a} \cup \bar{b''}) = -\delta(\overline{a \otimes b''}) ,$$

where, for the last equality, we have applied the previous lemma. Let b' be a preimage of b'' in B'. Then, we can calculate $\delta(\overline{a \otimes b''})$ as the class of $\mathrm{Nm}_G(a \otimes b')$ in $H_T^0(G, B)$. On the other hand, since $\bar{\varphi} = \delta b''$, we know that $\varphi(g) = gb' - b'$ for all $g \in G$. Then, we have

$$\mathrm{Nm}_G(a \otimes b') = \sum_{g \in G} ga \otimes gb' = \sum_{g \in G} ga \otimes \varphi(g) - \sum_{g \in G} ga \otimes b' = \sum_{g \in G} ga \otimes \varphi(g) - \mathrm{Nm}_G a \otimes b = -c ,$$

and the desired result follows. □

Lemma 3.3.4. Let G be a finite group and let B be a G-module. Let $\varphi : G \to B$ be a 1-cocycle, and let $\bar{\varphi}$ denote its class in $H_T^1(G, B)$. For any $x \in G$, let $\bar{x}$ be the image of its class in $G^{\mathrm{ab}} = G/G^c$ under the isomorphism $G^{\mathrm{ab}} \simeq H_T^{-2}(G, \mathbb{Z})$ from Proposition 1.9.2. Then, for any $x \in G$,

$$\bar{x} \cup \bar{\varphi} = \overline{\varphi(x)} \in H_T^{-1}(G, B) .$$

Proof. Consider the short exact sequence

$$0 \longrightarrow I_G \otimes B \longrightarrow \mathbb{Z}[G] \otimes B \longrightarrow B \longrightarrow 0$$

resulting from tensoring the augmentation sequence with B. Since $\mathbb{Z}[G] \otimes B$ is induced, the connecting map

$$\delta : H_T^{-1}(G, B) \to H_T^0(G, I_G \otimes B)$$

is an isomorphism. Therefore, in order to prove the desired identity it suffices to prove that, for any $x \in G$,

$$\delta(\bar{x} \cup \bar{\varphi}) = \delta(\overline{\varphi(x)}) \,.$$

A preimage of $\varphi(x)$ in $\mathbb{Z}[G] \otimes B$ is simply $1 \otimes \varphi(x)$, so that $\delta(\varphi(x))$ can be obtained as the class of $\mathrm{Nm}_G(1 \otimes \varphi(x))$ in $H_T^0(G, I_G \otimes B)$, i.e., as the class of

$$c = \mathrm{Nm}_G(1 \otimes \varphi(x)) = \sum_{g \in G} g \otimes g\varphi(x) \,.$$

Let $\bar{i_x} \in H_T^{-1}(G, I_G)$ be the image of $\bar{x}$ under the connecting map induced by the augmentation sequence. From the proof of the isomorphism $G^{\mathrm{ab}} \simeq H_T^{-2}(G, \mathbb{Z})$, this element is precisely the class of $x - 1 \in I_G$ in $H_T^{-1}(G, I_G)$.

We have

$$\delta(\bar{x} \cup \bar{\varphi}) = \bar{i_x} \cup \bar{\varphi} \,,$$

and, by he previous lemma, this is the class of the element

$$\begin{aligned} c' &= -\sum_{g \in G} g(x-1) \otimes \varphi(g) = -\sum_{g \in G} gx \otimes \varphi(g) + \sum_{g \in G} g \otimes \varphi(g) = \\ &= -\sum_{g \in G} gx \otimes \varphi(gx) + \sum_{g \in G} gx \otimes g\varphi(x) + \sum_{g \in G} g \otimes \varphi(g) = \sum_{g \in G} gx \otimes g\varphi(x) \,. \end{aligned}$$

Finally, we have

$$c - c' = \sum_{g \in G} g(1-x) \otimes g\varphi(x) = \mathrm{Nm}_G((1-x) \otimes \varphi(x)) \,,$$

which shows that c and c' represent the same element in $H_T^0(I_G \otimes B)$. □

Proposition 3.3.5. Assume that L/K is a finite Galois extension and define $G = \mathrm{Gal}(L/K)$. Let $\chi \in \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z}) = H^1(G, \mathbb{Q}/\mathbb{Z})$ be a character, and let $\delta\chi$ be its image by the connecting map $\delta : H^1(G, \mathbb{Q}/\mathbb{Z}) \to H^2(G, \mathbb{Z})$ obtained from the short exact sequence

$$0 \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Q} \longrightarrow \mathbb{Q}/\mathbb{Z} \longrightarrow 0 \,.$$

For any $\alpha \in K^\times$, let $\bar{\alpha}$ denote its image in $K^\times / \mathrm{Nm}_{L/K} L^\times$.

Then, for all $\alpha \in K^\times$,

$$\chi(\phi_{L/K}(\alpha)) = \mathrm{inv}_K(\bar{\alpha} \cup \delta\chi) \,.$$

Proof. Let $n = [L : K]$. By the definition of $\phi_{L/K}$, we have $\phi_{L/K}(\alpha) \cup u_{L/K} = \bar{\alpha}$, where we have identified $\phi_{L/K}(\alpha)$ with its image in $H^{-2}(G, \mathbb{Z})$ under the isomorphism $G^{\mathrm{ab}} \simeq H^{-2}(G, \mathbb{Z})$. Therefore, we have

$$\bar{\alpha} \cup \delta\chi = (\phi_{L/K}(\alpha) \cup u_{L/K}) \cup \delta\chi = (u_{L/K} \cup \phi_{L/K}(\alpha)) \cup \delta\chi = u_{L/K} \cup (\phi_{L/K}(\alpha) \cup \delta\chi) \,,$$

where the second equality holds because $\phi_{L/K}(\alpha) \in H^{-2}(G,\mathbb{Z})$. Also because of this fact we have $\phi_{L/K}(\alpha) \cup \delta\chi = \delta(\phi_{L/K}(\alpha) \cup \chi)$. Observe that here $\phi_{L/K}(\alpha) \cup \chi \in H^{-1}(G,\mathbb{Q}/\mathbb{Z})$, and the connecting map

$$\frac{1}{n}\mathbb{Z}/\mathbb{Z} = H^{-1}(G,\mathbb{Q}/\mathbb{Z}) \to H^0_T(G,\mathbb{Z}) = \mathbb{Z}/n\mathbb{Z}$$

is multiplication by $|G| = n$ (because the action is trivial). By the previous lemma, we have $\phi_{L/K}(\alpha) \cup \chi = \chi(\phi_{L/K}(\alpha))$. Altogether, if $\chi(\phi_{L/K}(\alpha)) = r/n$, with $r \in \mathbb{Z}$, we get

$$\bar{\alpha} \cup \delta\chi = r \cdot u_{L/K}\,,$$

and the result follows by applying the invariant map inv_K on both sides. □

Theorem 3.3.6. (Reciprocity Law) There exists a homomorphism

$$\phi_K : K^\times \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$$

such that:

1. for every prime π, we have $\phi_K(\pi)|_K^{\mathrm{un}} = \mathrm{Frob}_K$.
2. for every finite Abelian extension L/K, the map

$$K^\times \xrightarrow{a \mapsto \phi_K(a)|_L} \mathrm{Gal}(L/K)$$

has kernel $\mathrm{Nm}_{L/K}L^\times$.

Proof. We will prove that the maps $\phi_{L/K}$ previously defined are compatible, in the sense that, if L and M are finite Galois extensions of K with Galois groups H and G, respectively, and with $L \subseteq M$, then the diagram

$$\begin{array}{ccc} K^\times & \xrightarrow{\phi_{M/K}} & G^{\mathrm{ab}} \\ \Big\downarrow{=} & & \Big\downarrow{\sigma \mapsto \sigma|_L} \\ K^\times & \xrightarrow{\phi_{L/K}} & H^{\mathrm{ab}} \end{array}$$

commutes. To that end, let $\chi \in \mathrm{Hom}(H,\mathbb{Q}/\mathbb{Z})$ be a character and let $\chi' \in \mathrm{Hom}(G,\mathbb{Q}/\mathbb{Z})$ be the character obtained from χ through the composite

$$G \to G/\mathrm{Gal}(M/L) = H \xrightarrow{\chi} \mathbb{Q}/\mathbb{Z}\,.$$

For any $\alpha \in K^\times$, let s_α be a representative of $\phi_{L/K}(\alpha)$ in H (thinking of H^{ab} as H/H^c), let s'_α be a representative of $\phi_{M/K}(\alpha)$ in G (thinking of G^{ab} as G/G^c), and let $\bar{\alpha}$ and $\bar{\alpha}'$ be the images of α in $K^\times/\mathrm{Nm}_{L/K}L^\times$ and $K^\times/\mathrm{Nm}_{M/K}M^\times$, respectively. Then, taking into account the previous proposition, we have, for all $\alpha \in K^\times$,

$$\chi(s'_\alpha|_L) = \chi'(s'_\alpha) = \mathrm{inv}_K(\bar{\alpha}' \cup \delta\chi') = \mathrm{inv}_K(\mathrm{Inf}(\bar{\alpha} \cup \delta\chi)) = \mathrm{inv}_K(\bar{\alpha} \cup \delta\chi) = \chi(s_\alpha)\,.$$

Since this is true for all $\chi \in \mathrm{Hom}(H,\mathbb{Q}/\mathbb{Z})$, we deduce that $s_\alpha^{-1}s'_\alpha|_L \in H^c$ and, consequently, that $\phi_{M/K}(\alpha)$ equals $\phi_{L/K}(\alpha)$ in H^{ab}.

Because of the compatibility of the maps $\phi_{L/K}$, we can define a map

$$\phi_K : K^\times \to \varprojlim \mathrm{Gal}(L/K)^{\mathrm{ab}} = \mathrm{Gal}(K^{\mathrm{ab}}/K)\,.$$

It satisfies the second property in the statement because of the definition of the maps $\phi_{L/K}$. To prove that it satisfies the first property, we need only prove that for all prime π and all finite unramified extension L/K we have $\phi_{L/K}(\pi) = \mathrm{Frob}_{L/K}$. But this is a direct consequence of Proposition 3.1.9. □

Lemma 3.3.7. Let E be a finite separable extension of K. Then, we have the following commutative diagrams:

$$\begin{array}{ccc} E^\times & \xrightarrow{\phi_E} & \mathrm{Gal}(K^s/E)^{\mathrm{ab}} \\ \downarrow{\scriptstyle \mathrm{Nm}_{E/K}} & & \downarrow{\scriptstyle i} \\ K^\times & \xrightarrow{\phi_K} & \mathrm{Gal}(K^s/K)^{\mathrm{ab}} \end{array} \qquad \begin{array}{ccc} K^\times & \xrightarrow{\phi_K} & \mathrm{Gal}(K^s/K)^{\mathrm{ab}} \\ \downarrow{\scriptstyle i} & & \downarrow{\scriptstyle \mathrm{Ver}} \\ E^\times & \xrightarrow{\phi_E} & \mathrm{Gal}(K^s/E)^{\mathrm{ab}} \end{array},$$

where i denotes in the first diagram the homomorphism induced by the inclusion $\mathrm{Gal}(K^s/E) \hookrightarrow \mathrm{Gal}(K^s/K)$ and in the second diagram the inclusion $K^\times \overset{E}{\hookrightarrow}{}^\times$.

Proof. Let L be a finite Galois extension of K containing E. Then, from Lemma 3.2.11 we know that $\mathrm{Res}(u_{L/K}) = u_{L/E}$. Therefore, we can see that, for any $r \in \mathbb{Z}$, the diagram

$$\begin{array}{ccc} H_T^r(\mathrm{Gal}(L/E), \mathbb{Z}) & \xrightarrow{\cup u_{L/E}} & H_T^{r+2}(\mathrm{Gal}(L/E), L^\times) \\ \downarrow{\scriptstyle \mathrm{Cor}} & & \downarrow{\scriptstyle \mathrm{Cor}} \\ H_T^r(\mathrm{Gal}(L/K), \mathbb{Z}) & \xrightarrow{\cup u_{L/K}} & H_T^{r+2}(\mathrm{Gal}(L/K), L^\times) \end{array}$$

commutes by means of the property

$$\mathrm{Cor}(x \cup u_{L/E}) = \mathrm{Cor}(x \cup \mathrm{Res}(u_{L/K})) = \mathrm{Cor}(x) \cup u_{L/K} \quad \text{for all } x \in H_T^r(\mathrm{Gal}(L/E), \mathbb{Z}).$$

Combining the commutative diagram obtained in the case $r = -2$ with the commutative diagram from Proposition 1.9.2 and the commutative diagram (1.2), we get the commutative diagram

$$\begin{array}{ccc} E^\times & \xrightarrow{\phi_{L/E}} & \mathrm{Gal}(L/E)^{\mathrm{ab}} \\ \downarrow{\scriptstyle \mathrm{Nm}_{E/K}} & & \downarrow{\scriptstyle i} \\ K^\times & \xrightarrow{\phi_{L/K}} & \mathrm{Gal}(L/K)^{\mathrm{ab}} \end{array},$$

and the first diagram in the statement is obtained by taking projective limits.

In a similar way, given a Galois extension L/K containing E, the diagrams

$$\begin{array}{ccc} H_T^r(\mathrm{Gal}(L/K), \mathbb{Z}) & \xrightarrow{\cup u_{L/K}} & H_T^{r+2}(\mathrm{Gal}(L/K), L^\times) \\ \downarrow{\scriptstyle \mathrm{Res}} & & \downarrow{\scriptstyle \mathrm{Res}} \\ H_T^r(\mathrm{Gal}(L/E), \mathbb{Z}) & \xrightarrow{\cup u_{L/E}} & H_T^{r+2}(\mathrm{Gal}(L/E), L^\times) \end{array}$$

commute for all $r \in \mathbb{Z}$ because of the property

$$\mathrm{Res}(x \cup u_{L/K}) = \mathrm{Res}(x) \cup \mathrm{Res}(u_{L/K}) = \mathrm{Res}(x) \cup u_{L/E} \quad \text{for all } x \in H_T^r(\mathrm{Gal}(L/E), \mathbb{Z}).$$

Combining the commutative diagram obtained in the case $r = -2$ with the commutative diagram from Proposition 1.9.6 we obtain a commutative diagram

$$\begin{array}{ccc} K^\times & \xrightarrow{\phi_{L/K}} & \mathrm{Gal}(L/K)^{\mathrm{ab}} \\ \downarrow{\scriptstyle i} & & \downarrow{\scriptstyle \mathrm{Ver}} \\ E^\times & \xrightarrow{\phi_{L/E}} & \mathrm{Gal}(L/E)^{\mathrm{ab}} \end{array},$$

and the second commutative diagram in the statement follows by taking projective limits. □

Theorem 3.3.8. (Norm limitation theorem) Assume that L/K is a finite separable extension, and let E be the maximal Abelian subextension of L/K. Then,

$$\mathrm{Nm}_{L/K} L^\times = \mathrm{Nm}_{E/K} E^\times .$$

Proof. By the transitivity of the norms, it is clear that $\mathrm{Nm}_{L/K} L^\times \subseteq \mathrm{Nm}_{E/K} E^\times$, so we will focus on proving the inclusion $\mathrm{Nm}_{E/K} E^\times \subseteq \mathrm{Nm}_{L/K} L^\times$. Let L' be a Galois extension of K containing L. Define $G = \mathrm{Gal}(L'/K)$ and $H = \mathrm{Gal}(L'/L)$. Since E is the maximal Abelian of K contained in L, the subgroup of G fixing it is $G^c H$. We have a commutative diagram

$$\begin{array}{ccc} L^\times & \xrightarrow{\phi_{L'/L}} & H/H^c \\ \downarrow{\scriptstyle \mathrm{Nm}_{L/K}} & & \downarrow{\scriptstyle i} \\ K^\times & \xrightarrow{\phi_{L'/K}} & G/G^c \\ \downarrow{\scriptstyle =} & & \downarrow \\ K^\times & \xrightarrow{\phi_{E/K}} & G/G^c H \end{array}$$

(the first square commutes because of the previous lemma and the second square commutes because of the compatibility property proved in Theorem 3.3.6).

Now, for any $a \in \mathrm{Nm}_{E/K} E^\times$, we know that $\phi_{E/K}(a) = 1$, so that $\phi_{L'/K}(a) \in G^c H/G^c$. Thus, since $\phi_{L'/L} : L^\times \to H/H^c$ is surjective, there exists some $b \in L^\times$ such that $i(\phi_{L'/L}(b)) = \phi_{L'/K}(a)$ and, in view of the commutativity of the diagram, we have $\phi_{L'/K}(\mathrm{Nm}_{L/K} b) = \phi_{L'/K}(a)$. This implies that $a = \mathrm{Nm}_{L/K} b \cdot \mathrm{Nm}_{L'/K} c$ for some $c \in L'$, and, because of the transitivity of the norms, we clearly see that $a \in \mathrm{Nm}_{L/K} L^\times$. □

Corollary 3.3.9. For every finite separable extension L/K, the group $\mathrm{Nm}_{L/K} L^\times$ is an open subgroup of $K^\times$.

Proof. Because of the previous theorem and Theorem 3.3.6, we see that $\mathrm{Nm}_{L/K} L^\times$ has finite index in $K^\times$. Thinking about valuations, we easily deduce that $\mathrm{Nm}_{L/K} L^\times \cap U_K = \mathrm{Nm}_{L/K} U_L$, so that we get an injective homomorphism $U_K/\mathrm{Nm}_{L/K} U_L \hookrightarrow K^\times/\mathrm{Nm}_{L/K} L^\times$ which shows that $\mathrm{Nm}_{L/K} U_L$ has finite index in U_K. On the other hand, since U_L is a compact subgroup of $L^\times$ and the norm map is continuous, we see that $\mathrm{Nm}_{L/K} U_L$ is compact and hence closed in $K^\times$. Therefore $\mathrm{Nm}_{L/K} U_L$ is a closed subgroup of finite index of U_K, which is compact, so that $\mathrm{Nm}_{L/K} U_L$ is an open subgroup of U_K. Since U_K is itself open in $K^\times$, we conclude that $\mathrm{Nm}_{L/K} U_L$ is open in $K^\times$ and hence that $\mathrm{Nm}_{L/K} L^\times$ is open in $K^\times$. □

Chapter 4

Idèles

Throughout this chapter, K will denote a number field. Given a prime of K, we will use the notation K_v to denote its completion with respect to v, and we will use U_v to denote $\mathcal{O}_v$, if v is finite, and $K_v^\times$, if v is infinite.

4.1 Definitions and main properties

References: [Mil13], [Neu99].

Definition 4.1.1. An *idèle of* K is an element in $\prod_v K_v^\times$, where v runs through all the primes of K, such that $\alpha_v \in U_v$ for all but finitely many primes.

With the product defined componentwise, it is clear that the idèles of K form a group, which we will call the *idèle group of* K and we will denote by $\mathbb{I}_K$.

We define a topology in $\mathbb{I}_K$ by taking as a basic system of neighborhoods the sets of the form

$$\prod_{v\in S} W_v \times \prod_{v\notin S} U_v\,,$$

where S is a finite set of primes and, for each $v \in S$, the set W_v is an open subset of $K_v^\times$.

It is straightforward that in fact this construction defines a topology on $\mathbb{I}_K$ and that, with this topology, both the product and taking inverses are continuous maps, so that $\mathbb{I}_K$ becomes a topological group. Moreover, $\mathbb{I}_K$ is locally compact. To see this, observe that, for $\alpha = (\alpha_v) \in \mathbb{I}_K$, with $\alpha_v \in \mathcal{O}_v^\times$ for all $v \notin S$, where S is a finite set of primes,

$$\prod_{v\in S} K_v^\times \times \prod_{v\notin S} U_v$$

is a locally compact neighborhood of α, since it is the product of compact spaces and finitely many locally compact spaces (for this set, the topology as a subgroup of the idèle group coincides with the product topology).

The locally compact sets

$$\prod_{v\in S} K_v^\times \times \prod_{v\notin S} U_v\,,$$

(where S is a finite set of primes) are open subgroups of $\mathbb{I}_K$. Their elements are called *S-idèles* and we will denote these subgroups by $\mathbb{I}_K^S$.

For each prime v, the field K can be canonically embedded into the completion K_v. Then, we have the following canonical diagonal embedding:

$$\begin{aligned} K^\times &\to \mathbb{I}_K \\ a &\mapsto (\alpha_v),\ \alpha_v = a \text{ for all prime } v\,. \end{aligned}$$

The elements in the image of this embedding are called *principal idèles*. We will denote the subgroup of principal idèles also by $K^\times$.

Lemma 4.1.2. $K^\times$ is a discrete (closed) subgroup of $\mathbb{I}_K$.

Proof. Let S_∞ stand for the set of infinite primes of K (which is clearly finite as there are finitely many embeddings of a number field into an algebraically closed field). Define the set $\mathcal{U}$ in the following way:

$$\mathcal{U} = \{\alpha \in \mathbb{I}_K : |\alpha_v|_v = 1\ \forall v \notin S_\infty,\ |\alpha_v - 1|_v < 1\ \forall v \in S_\infty\}\,;$$

that is,

$$\mathcal{U} = \prod_{v\in S_\infty} W_v^\times \times \prod_{v\notin S_\infty} U_v^\times\,,$$

where

$$W_v = \{\alpha_v \in K_v^\times : |\alpha_v - 1|_v < 1\}\,.$$

It is clear that, with the topology which we have defined on $\mathbb{I}_K$, the set $\mathcal{U}$ is an open neighborhood of 1.

Let us prove that $\mathcal{U}$ does not contain any other principal idèle. Suppose that a were a principal idèle in $\mathcal{U}$ different from 1. Then, the product formula (Proposition 2.6.2) applied to $a-1$ gives

$$1 = \prod_v |a-1|_v = \prod_{v\in S_\infty} |a-1|_v \prod_{v\notin S_\infty} |a-1|_v < \prod_{v\notin S_\infty} |a-1|_v \leqslant \prod_{v\notin S_\infty} \max\{|a|_v, 1\} = 1\,,$$

which is a contradiction.

Since $\mathbb{I}_K$ is a topological group, the map $(x,y)\mapsto xy^{-1}$ is continuous, and, consequently, there exists an open neighborhood $\mathcal{V}$ of 1 such that $\mathcal{V}\mathcal{V}^{-1}\subseteq\mathcal{U}$. Then, for any principal idèle a, the set $a\mathcal{V}$ is an open neighborhood of a not containing any other principal idèle, as, if ax were a different principal idèle in $a\mathcal{V}$, then $x = axa^{-1}\in\mathcal{U}$ would be a principal idèle in $\mathcal{U}$ different from 1. □

Definition 4.1.3. The *idèle class group* of K is the quotient group

$$C_K = \mathbb{I}_K/K^\times\,.$$

Let I_K denote the group of fractional ideals of K and let Cl_K denote the ideal class group of K. There is a canonical surjective homomorphism from the idèle group to the group of fractional ideals:

$$\begin{aligned} \mathrm{id} : \mathbb{I}_K &\to I_K \\ \alpha = (\alpha_v) &\mapsto \prod_{v \text{ finite}} \mathfrak{p}_v^{\mathrm{ord}_v(\alpha_v)}\,. \end{aligned}$$

The kernel of this map is clearly $\mathbb{I}_K^{S_\infty}$. Observe that any principal idèle ($a\in K^\times$) maps to a principal fractional ideal ($a\mathcal{O}_K$) and, consequently, the previous map induces a surjective homomorphism

$$C_K \to Cl_K$$

whose kernel is $\mathbb{I}_K^{S_\infty}K^\times/K^\times$.

Lemma 4.1.4. Let S be a set of primes of K containing all infinite primes and a set of generators of the ideal class group of K. Then,

$$\mathbb{I}_K = \mathbb{I}_K^S K^\times .$$

Proof. Let J be the subgroup of I_K generated by the finite primes in S. The fact that these primes generate Cl_K means that every ideal $\mathfrak{a} \in I_K$ can be written as $a\mathfrak{b}$, with $a \in K^\times$ and $\mathfrak{b} \in J$.

Let $\alpha = (\alpha_v)_v \in \mathbb{I}_K$, and consider its image under the map id, i.e. $\mathfrak{a} = \prod_{v \text{ finite}} \mathfrak{p}_v^{\mathrm{ord}_v(\alpha_v)}$. It can be written as $\mathfrak{a} = a\mathfrak{b}$ for some $a \in K^\times$ and $\mathfrak{b} \in J$. Define $\alpha' = a^{-1}\alpha$. Since its image under the map id is $\mathfrak{b}$, which lies in J, we see that $\mathrm{ord}_v(\alpha) = 0$ for all finite prime out of S, which proves that $\alpha' \in \mathbb{I}_K^S$, and so $\alpha = a\alpha' \in \mathbb{I}_K^S K^\times$. □

4.2 The norm map

References: [Mil13]

Let L be a finite extension of K. We know that, for any prime v of K, and any prime $w|v$ of L, there are natural embeddings of K_v and L into L_w, and that the map

$$L \otimes_K K_v \to \prod_{w|v} L_w$$

defined by $a \otimes_K b \mapsto (ab)_{w|v}$ (with the natural embeddings) is an isomorphism of K_v-vector spaces (Proposition 2.5.2).

From this isomorphism, we get that, for any $a \in L$,

$$\mathrm{Nm}_{L/K}(a) = \prod_{w|v} \mathrm{Nm}_{L_w/K_v}(a) \tag{4.1}$$

(Corollary 2.5.3).

Definition 4.2.1. Let L/K be a finite extension of number fields. Then, the *idèle norm map*

$$\mathrm{Nm}_{L/K} : \mathbb{I}_L \to \mathbb{I}_K$$

is the map sending an idèle $\alpha = (\alpha_w)_w$ in $\mathbb{I}_L$ to the idèle $\beta = (\beta_v)_v$ defined by

$$\beta_v = \prod_{w|v} \mathrm{Nm}_{L_w/K_v}(\alpha_w) .$$

Lemma 4.2.2. We have the following commutative diagram:

$$\begin{array}{ccccc} L^\times & \longrightarrow & \mathbb{I}_L & \longrightarrow & I_L \\ \downarrow{\scriptstyle \mathrm{Nm}_{L/K}} & & \downarrow{\scriptstyle \mathrm{Nm}_{L/K}} & & \downarrow{\scriptstyle \mathrm{Nm}_{L/K}} \\ K^\times & \longrightarrow & \mathbb{I}_K & \longrightarrow & I_K \end{array} .$$

Proof. The first square is commutative as a consequence of (4.1). For the second square, take $\alpha = (\alpha_w)_w \in \mathbb{I}_L$. By applying the idèle norm map and then going to the right, we get:

$$\prod_{v \text{ finite}} \mathfrak{p}_v^{\mathrm{ord}_v\left(\prod_{w|v} \mathrm{Nm}_{L_w/K_v}\alpha_w\right)} = \prod_{v \text{ finite}} \mathfrak{p}_v^{\sum_{w|v} \mathrm{ord}_v\left(\mathrm{Nm}_{L_w/K_v}\alpha_w\right)} .$$

If we start going to the right and then we apply the ideal norm map, we get:

$$\prod_{v \text{ finite}} \prod_{w|v} \mathfrak{p}_v^{f_{w|v}\mathrm{ord}_w(\alpha_w)} = \prod_{v \text{ finite}} \mathfrak{p}_v^{\sum_{w|v} f_{w|v}\mathrm{ord}_w(\alpha_w)} .$$

Since K_v is complete, the valuation w is the unique extension of v to L_w, so that it satisfies:

$$\frac{\mathrm{ord}_w(\gamma)}{e_{w|v}} = \frac{1}{[L_w : K_v]}\mathrm{ord}_v\left(\mathrm{Nm}_{L_w/K_v}(\gamma)\right) \quad \forall \gamma \in L_w$$

(see Proposition 2.2.12) or, equivalently

$$f_{w|v}\mathrm{ord}_w(\gamma) = \mathrm{ord}_v\left(\mathrm{Nm}_{L_w/K_v}(\gamma)\right) ,$$

whereby commutativity follows. □

Remark 25. The previous commutative diagram induces the following commutative diagram:

$$\begin{array}{ccc} C_L & \longrightarrow & Cl_L \\ \downarrow{\scriptstyle \mathrm{Nm}_{L/K}} & & \downarrow{\scriptstyle \mathrm{Nm}_{L/K}} \\ C_K & \longrightarrow & Cl_K \end{array} .$$

Proposition 4.2.3. The quotient map $\mathbb{I}_K \to C_K$ induces an isomorphism

$$\mathbb{I}_K/K^\times \cdot \mathrm{Nm}_{L/K}\mathbb{I}_L \to C_K/\mathrm{Nm}_{L/K}C_L .$$

Proof. Consider the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & L^\times & \longrightarrow & \mathbb{I}_L & \longrightarrow & C_L & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathrm{Nm}_{L/K}} & & \downarrow{\scriptstyle \mathrm{Nm}_{L/K}} & & \downarrow{\scriptstyle \mathrm{Nm}_{L/K}} & & \\ 0 & \longrightarrow & K^\times & \longrightarrow & \mathbb{I}_K & \longrightarrow & C_K & \longrightarrow & 0 \end{array} .$$

The last part of the exact sequence given by the extended snake's lemma is:

$$K^\times/\mathrm{Nm}_{L/K}L^\times \to \mathbb{I}_K/\mathrm{Nm}_{L/K}\mathbb{I}_L \to C_K/\mathrm{Nm}_{L/K}C_L \to 0 .$$

This exact sequence gives us the desired isomorphism. □

Proposition 4.2.4. For a finite extension of number fields L/K, the group $\mathrm{Nm}_{L/K}\mathbb{I}_L$ is an open subgroup of $\mathbb{I}_K$.

Proof. For infinite primes v, we know that K_v is isomorphic to either $\mathbb{R}$ or $\mathbb{C}$. If it is isomorphic to $\mathbb{C}$, so is L_w for all $w|v$, and $\mathrm{Nm}_{L_w/K_v} L_w^\times = K_v^\times$. If $K_v \simeq \mathbb{R}$, then for any $w|v$, the extension L_w is isomorphic to either $\mathbb{R}$ or $\mathbb{C}$, so that $\mathrm{Nm}_{L_w/K_v} = K_v^\times$ or $\mathrm{Nm}_{L_w/K_v} = \mathbb{R}^+$.

For finite unramified primes v, the extension L_w/K_v is unramified for all $w|v$, so that, by Proposition 3.1.2, we have $\mathrm{Nm}_{L_w/K_v} U_w^\times = U_v^\times$.

Since $\mathrm{Nm}_{L_w/K_v} L_w^\times$ is always an open subgroup of $K_v^\times$ because of Corollary 3.3.9, for every finite ramified prime we have $1 + \mathfrak{p}_v^{m_v} \subseteq \mathrm{Nm}_{L_w/K_v} L_w^\times$ for some $m_v \in \mathbb{N}$.

Since there is a finite number of infinite primes and ramified finite primes, the previous observations yield the desired result. □

4.3 The cohomology of idèles

References: [Mil13]

Assume that L/K is a finite Galois extension, and let $G = \mathrm{Gal}(L/K)$. We know that, given a prime v of K, the group G acts transitively on the primes of L lying over v (Proposition 2.5.5). This action is defined by:

$$(\sigma, w) \mapsto \sigma w = w \circ \sigma^{-1} .$$

For a prime $w_0|v$ of L, the corresponding stabilizer is its decomposition group G_{w_0}, so that we get a bijection:

$$G/G_{w_0} \to \{w \in \mathrm{Spec}(\mathcal{O}_L) : w|v\} .$$

Since the map

$$\sigma : (L, |\cdot|_w) \to (L, |\cdot|_{\sigma w})$$

clearly preserves valuations, it can be extended to the corresponding completions:

$$\hat{\sigma} : (L_w, |\cdot|_w) \to (L_{\sigma w}, |\cdot|_{\sigma w}) .$$

The extended map is in fact a homeomorphism and a K_v-isomorphism, since it fixes K_v by continuity.

We can define an action of G on $\prod_{w|v} L_w$ through the isomorphism:

$$L \otimes_K K_v \simeq \prod_{w|v} L_w .$$

Let $L = K(\alpha)$ (since L/K is finite and separable, there exists such an α), let $f(X) \in K[X]$ be its minimal polynomial over K, and, for each $w|v$, let $f_w(X)$ the corresponding irreducible factor of $f(X)$ (*Remark* 18). Then, from the proof of the previous isomorphism, we have the chain of isomorphisms

$$L \otimes_K K_v \simeq K_v[X]/(f(X)) \simeq \prod_{w|v} K_v[X]/(f_w(X)) \simeq \prod_{w|v} L_w ,$$

from which we can easily see that the elements of G act continuously on $\prod_{w|v} L_w$ by studying their action on $K_v[X]/(f(X))$ and then taking it to $\prod_{w|v} L_w$. Moreover, it is clear that, for any $a \in L$, $\sigma(i_w(a))_w = (i_w(\sigma a))_w$. In fact, we have the following lemma:

Lemma 4.3.1. The action of G on $\prod_{w|v} L_w$ defined through the isomorphism

$$L \otimes_K K_v \simeq \prod_{w|v} L_w$$

is the unique continuous action of G on $\prod_{w|v} L_w$ which satisfies that, for any $a \in L$,

$$\sigma(i_w(a))_w = (i_w(\sigma a))_w \,.$$

Proof. Taking into account the weak approximation theorem, any continuous map

$$\sigma : \prod_{w|v} L_w \to \prod_{w|v} L_w$$

is determined by its action on the elements of the form $(i_w(a))_w$ for some $a \in L$. □

The following lemma provides an explicit formula for the action of G on $\prod_{w|v} L_w$.

Lemma 4.3.2. The action previously defined satisfies:

$$\sigma((\alpha_w)_w) = (\sigma\alpha_w)_{\sigma w} \,,$$

where, on the right hand side, σ denotes, in each case, the corresponding extension of

$$\sigma : (L, |\cdot|_w) \to (L, |\cdot|_{\sigma w})$$

to the completions:

$$\hat{\sigma} : (L_w, |\cdot|_w) \to (L_{\sigma w}, |\cdot|_{\sigma w}) \,.$$

Proof. It is clear that this action is continuous, and it is straightforward to check that it satisfies the property from the previous lemma. □

Remember that we have an isomorphism

$$G_w \simeq \mathrm{Gal}(L_w/K_v)$$

(Proposition 2.5.9), so that we can consider L_w as G_w-module.

Proposition 4.3.3. Let v be a prime of K and let w_0 be a prime of L over v. Then, for any $\alpha \in \prod_{w|v} L_w$, the map $f_\alpha : G \to L_{w_0}$ defined by $f_\alpha(\sigma) = \sigma(\alpha_{\sigma^{-1}w_0})$ belongs to $\mathrm{Ind}_{G_{w_0}}^G(L_{w_0})$, and the map:

$$\begin{aligned} \prod_{w|v} L_w &\to \mathrm{Ind}_{G_{w_0}}^G(L_{w_0}) \\ \alpha &\mapsto f_\alpha \end{aligned}$$

is an isomorphism of G-modules.

Proof. Let $\alpha \in \prod_{w|v} L_w$. Then, for any $\tau \in G_{w_0}$,

$$f_\alpha(\tau\sigma) = \tau\sigma(\alpha_{\sigma^{-1}\tau^{-1}w_0}) = \tau\sigma(\alpha_{\sigma^{-1}w_0}) = \tau f_\alpha(\sigma) \,,$$

which proves that $f_\alpha \in \mathrm{Ind}_{G_{w_0}}^G(L_{w_0})$. Now, observe that

$$f_{\alpha+\beta}(\sigma) = \sigma((\alpha+\beta)_{\sigma^{-1}w_0}) = \sigma(\alpha_{\sigma^{-1}w_0}) + \sigma(\beta_{\sigma^{-1}w_0}) = f_\alpha(\sigma) + f_\beta(\sigma)$$

and, for any $\tau \in G$,

$$f_{\tau\alpha}(\sigma) = \sigma((\tau\alpha)_{\sigma^{-1}w_0}) = \sigma(\tau(\alpha_{\tau^{-1}\sigma^{-1}w_0})) = f_\alpha(\sigma\tau) = (\tau f_\alpha)(\sigma) \,,$$

so that the map $\alpha \mapsto f_\alpha$ is a homomorphism of G-modules. Finally, an inverse is given by $f \mapsto \alpha_f$, with $(\alpha_f)_{\sigma w_0} = \sigma(f(\sigma^{-1}))$. □

Proposition 4.3.4. With the previous definitions, we have

$$H^r(G, \prod_{w|v} L_w) \simeq H^r(G_{w_0}, L_{w_0})$$

for all $r \geqslant 0$ (and for all $\mathbb{Z}$ when we consider Tate cohomology).

Proof. Apply the previous proposition and Shapiro's lemma. □

Lemma 4.3.5. With the previous definitions, there are canonical isomorphisms between the groups $H^r(G_w, L_w)$ with $w|v$, satisfying that, if

$$\phi_{w,w'} : H^r(G_w, L_w) \to H^r(G_{w'}, L_{w'})$$

are such isomorphisms,

$$\phi_{w,w''} = \phi_{w',w''} \circ \phi_{w,w'} .$$

Proof. Given any two primes $w, w'|v$, since G acts transitively on the set of primes over v, we can find $\sigma \in G$ such that $w' = \sigma w$. The maps

$$\begin{aligned} \alpha : G_w &\to G'_w \\ \rho &\mapsto \sigma\rho\sigma^{-1} \end{aligned}$$

and

$$\begin{aligned} \beta : L'_w &\to L_w \\ x &\mapsto \sigma^{-1}x \end{aligned}$$

form a pair of compatible isomorphisms, so that they define an isomorphism

$$\phi_{w',w} : H^r(G_{w'}, L_{w'}) \to H^r(G_w, L_w) .$$

This isomorphism is independent of σ, since, if $w' = \sigma' w$, then $\sigma' = \sigma\tau$ for some $\tau \in G_w$, so that we would have found an isomorphism $\phi'_{w',w}$ differing from the previous one by an isomorphism

$$\phi_{w,w} : H^r(G_w, L_w) \to H^r(G_w, L_w)$$

obtained from τ in the same way; but $\phi_{w,w}$ is the identity because of Lemma 1.4.2. The fact that these isomorphisms satisfy

$$\phi_{w,w''} = \phi_{w',w''} \circ \phi_{w,w'}$$

is straightforward. □

Remark 26. We get results analogous to Proposition 4.3.3, Proposition 4.3.4 and Lemma 4.3.5 with $L_w^\times$ and U_w.

Taking into account the last lemma, when working with cohomology groups of the form $H^r(G_w, L_w)$, $H^r(G_w, L_w^\times)$ or $H^r(G_w, U_w)$, we will usually use the notation G^v, L^v and U^v to refer to G_w, L_w and U_w for any $w|v$.

For every prime v of K we have defined an action of G on $\prod_{w|v} L_w$. We can extend these actions to an action of G on $\mathbb{I}_L$. This action of G on $\mathbb{I}_L$ turns it into a G-module.

Proposition 4.3.6. With the action of G on $\mathbb{I}_L$ just defined:

1. The map
$$\begin{aligned} \mathbb{I}_K &\to \mathbb{I}_L \\ (\alpha_v)_v &\mapsto (\beta_w)_w, \text{ where } \beta_w = \alpha_v \text{ for } w|v \end{aligned}$$
induces an isomorphism
$$\mathbb{I}_K \simeq \mathbb{I}_L^G .$$

2. For all $r \in \mathbb{Z}$,
$$H^r(G, \mathbb{I}_L) = \bigoplus_v H^r(G^v, L^{v\times})$$
(considering Tate cohomology).

Proof. For the first statement, note that the given map is clearly injective, so we need only show that its image is $\mathbb{I}_L^G$, i.e. the set of elements of $\mathbb{I}_L$ fixed by G. Lemma 4.3.2 allows us to give an explicit description of the action of G: $(\alpha_w)_w$ is mapped to $(\sigma\alpha_w)_{\sigma w}$. Therefore, it is clear that G fixes the image of $\mathbb{I}_K$. Conversely, let $(\alpha_w)_w \in \mathbb{I}_L$ be fixed by G. Then, $\alpha_{\sigma w} = \sigma\alpha_w$ for all prime w of L and all $\sigma \in G$. In particular, we have that $\alpha_w = \tau\alpha_w$ for all $\tau \in G_w$, so that for each $w|v$, α_w is fixed by $\mathrm{Gal}(L_w/K_v)$, which implies $\alpha_w \in K_v$. Now, from the fact that G acts transitively on the set of valuations $w|v$ and the explicit formula for the action of G on $\prod_{w|v} L_w^\times$, we deduce that all α_w with $w|v$ correspond to the same $\alpha_v \in K_v$. We conclude that $(\alpha_w)_w$ is the image of an idèle $(\alpha_v)_v \in \mathbb{I}_K$.

For the second statement, observe that $\mathbb{I}_L$ can be regarded as the direct limit of the groups
$$\mathbb{I}_L^S = \prod_{v\in S}\prod_{w|v} L_w^\times \times \prod_{v\notin S}\prod_{w|v} U_w ,$$
where S runs through the finite sets of primes of K containing the infinite primes and the primes that ramify in L. Note that the groups $\mathbb{I}_L^S$ are stable under the action of G, so they are themselves G-modules. Let us calculate their cohomology groups:
$$\begin{aligned} H^r(G, \mathbb{I}_L^S) &= \prod_{v\in S} H^r(G, \prod_{w|v} L_w^\times) \times \prod_{v\notin S} H^r(G, \prod_{w|v} U_w) = \\ &= \prod_{v\in S} H^r(G^v, L^{v\times}) \times \prod_{v\notin S} H^r(G^v, U^v) = \prod_{v\in S} H^r(G^v, L^{v\times}) , \end{aligned}$$
where we have used that, for unramified primes v, we have $H^r(G^v, U^v) = 0$ (Proposition 3.1.3).

Then, using Proposition 1.8.4, we get
$$H^r(G, \mathbb{I}_L) = \varinjlim H^r(G, \mathbb{I}_L^S) = \varinjlim \prod_{v\in S} H^r(G^v, L^{v\times}) = \bigoplus_v H^r(G^v, L^{v\times}) .$$

□

Remark 27. As a consequence of the first part of the previous proposition, for a finite Galois extension, the idèle norm map previously defined can be viewed as the norm map defined in general for a G-module with finite G:
$$\begin{aligned} \mathrm{Nm}_{L/K} : \mathbb{I}_L &\to \mathbb{I}_K \\ \alpha &\mapsto \prod_{\sigma\in G} \sigma\alpha . \end{aligned}$$

Corollary 4.3.7. With the previous definitions:

1. $H^1(G, \mathbb{I}_L) = 0$.
2. $H^2(G, \mathbb{I}_L) = \bigoplus_v \left(\frac{1}{n_v}\mathbb{Z}/\mathbb{Z}\right)$, where $n_v = [L^v : K_v]$.

Proof. The first identity follows from Hilbert's theorem 90, whereas the second one follows from the isomorphism given by the invariant map (see the discussion preceding Lemma 3.2.10). □

Proposition 4.3.8. Let L/K be a finite cyclic extension. Let S be a finite set of primes of K containing the infinite primes. Then:

$$h(G, \mathbb{I}_L^S) = \prod_{v \in S} n_v \,,$$

where $n_v = [L^v : K_v]$.

Proof. We have that

$$h(G, \mathbb{I}_L^S) = \prod_{v \in S} h\left(G, \prod_{w|v} L_w^\times\right) \prod_{v \notin S} h\left(G, \prod_{w|v} U_w\right) = \prod_{v \in S} h(G^v, L^{v\times}) \prod_{v \notin S} h(G^v, U^v) \,,$$

and, by Lemma 3.2.5, we know that $h(G^v, L^{v\times}) = n_v$ for all v and $h(G^v, U^v) = 1$ for all finite v. □

Chapter 5

Idelic-theoretic global class field theory

5.1 Introduction

References: [Mil13]

Let K be a number field and let L be a finite Abelian extension of K. Then, for any prime v of K and for any prime $w|v$ of L, the extension L_w/K_v is a finite Abelian extension of local fields. For K_v, we have the local Artin map

$$\phi_v : K_v^\times \to \mathrm{Gal}(K_v^{\mathrm{ab}}/K_v)\,,$$

which provides a homomorphism

$$\begin{aligned}\phi_{L_w/K_v} : K_v^\times &\to \mathrm{Gal}(L_w/K_v)\\ a &\mapsto \phi_v(a)|_{L_w}\,.\end{aligned}$$

Because of the isomorphism

$$\begin{aligned}\mathrm{Gal}(L_w/K_v) &\to G_w\\ \sigma &\mapsto \sigma|_L\,,\end{aligned}$$

we get, then, a homomorphism

$$\phi_{v,L/K} : K_v^\times \to G_w \subseteq \mathrm{Gal}(L/K)\,.$$

The local Artin map is independent on the maximal Abelian extension K_v^{ab} of K_v, in the sense that, if $K_v^{\mathrm{ab},1}$ and $K_v^{\mathrm{ab},2}$ are two such extensions and

$$\rho : K_v^{\mathrm{ab},1} \to K_v^{\mathrm{ab},2}\,,$$

is any K_v-isomorphism between these extensions, then the corresponding Artin maps are related by

$$\phi_v^2(a) = \rho \circ \phi_v^1(a) \circ \rho^{-1} \quad \text{for all } a \in K_v^\times \tag{5.1}$$

(note that this relation does not depend on the choice of the isomorphism ρ, since we are working with Abelian extensions). In particular, if σw is any other prime of L dividing v, and we take

$K_v^{\mathrm{ab},1}$ and $K_v^{\mathrm{ab},2}$ to be maximal Abelian extensions of L_w and $L_{\sigma w}$, respectively, we can take ρ to be the extension to the maximal Abelian extensions of the isomorphism

$$\hat{\sigma} : L_w \to L_{\sigma w}$$

obtained extending by continuity the map

$$\sigma : (L, |\cdot|_w) \to (L, |\cdot|_{\sigma w}) .$$

Therefore, restricting the maps in (5.1) to L, we find that

$$\phi_v^2(a)|_L = \phi_v^1(a)|_L \quad \text{for all } a \in K_v^\times .$$

This proves that the map $\phi_{v,L/K}$ is independent of w, which justifies this notation.

Proposition 5.1.1. Let K be a number field. There exists a unique continuous map

$$\phi_K : \mathbb{I}_K \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$$

such that, for any finite Abelian extension $L \subseteq K^{\mathrm{ab}}$ of K, for any prime v of K and for any prime $w|v$ of L, the diagram

$$\begin{array}{ccc} K_v^\times & \xrightarrow{a \mapsto \phi_v(a)|_{L_w}} & \mathrm{Gal}(L_w/K_v) \\ \downarrow & & \downarrow \\ \mathbb{I}_K & \xrightarrow{\alpha \mapsto \phi_K(\alpha)|_L} & \mathrm{Gal}(L/K) \end{array}$$

is commutative.

Proof. Given an idèle $\alpha = (\alpha_v) \in \mathbb{I}_K$, we know that $\alpha_v \in U_v$ for all but finitely many primes v. We also know that, for any finite extension L of K, there are only finitely many primes of K which ramify in L. Altogether, we know that, for any finite Abelian extension L,

$$\phi_{v,L/K}(\alpha_v) = 1$$

for all but finitely many primes, as it occurs whenever v is unramified and α_v is a unit (for finite unramified primes, all units are norms). We can therefore define $\phi_{L/K}$ in the following way:

$$\phi_{L/K}(\alpha) = \prod_v \phi_{v,L/K}(\alpha_v) .$$

Let L' be another Abelian extension of K such that $L \subseteq L'$. Let $w|v$ be a prime of L and $w'|w$ a prime of L'. Then, from the fact that

$$\phi_{L_w/K_v}(a) = \phi_{L'_{w'}/K_v}(a)|_{L_w} \quad \text{for all } a \in K_v^\times ,$$

it easily follows that

$$\phi_{v,L/K}(a) = \phi_{v,L'/K}(a)|_L \quad \text{for all } a \in K_v^\times ,$$

and, consequently,

$$\phi_{L/K}(\alpha) = \phi_{L'/K}(\alpha)|_L \quad \text{for all } \alpha \in \mathbb{I}_K ,$$

Therefore, we can define a map

$$\phi_K : \mathbb{I}_K \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$$

such that

$$\phi_K(\alpha)|_L = \phi_{L/K}(a)$$

for all finite Abelian extension $L \subseteq K^{\mathrm{ab}}$.

It is obvious that this map is a homomorphism that makes the diagram

$$\begin{array}{ccc} K_v^\times & \xrightarrow{a \mapsto \phi_v(a)|_{L_w}} & \mathrm{Gal}(L_w/K_v) \\ \downarrow & & \downarrow \\ \mathbb{I}_K & \xrightarrow{\alpha \mapsto \phi_K(\alpha)|_L} & \mathrm{Gal}(L/K) \end{array}$$

commutative for all prime v of K and for all finite Abelian extension L. It remains to prove that it is continuous.

We know, from local class field theory, that $\mathrm{Nm}_{L_w/K_v}(L_w^\times) \subseteq \ker \phi_{L_w/K_v}$. Therefore,

$$\mathrm{Nm}_{L_w/K_v}(L_w^\times) \subseteq \ker \phi_{v,L/K}\,,$$

and, consequently,

$$\mathrm{Nm}_{L/K}\mathbb{I}_L \subseteq \ker \phi_{L/K}\,.$$

Since $\mathrm{Nm}_{L/K}\mathbb{I}_L$ is open in $\mathbb{I}_K$, this implies that

$$\phi_{L/K} : \mathbb{I}_K^\times \to \mathrm{Gal}(L/K)$$

is continuous. Then, since ϕ is the map

$$\mathbb{I}_K^\times \to \mathrm{Gal}(K^{\mathrm{ab}}/K) = \varprojlim \mathrm{Gal}(L/K)$$

obtained from the family of compatible maps $\phi_{L/K}$, it is also continuous.

To prove uniqueness, observe that, for all finite Abelian extension L, the condition on the commutativity of the diagrams uniquely determines $\phi_{L/K}$ on the idèles α with $\alpha_v = 1$ for all but finitely many primes v. The continuity of ϕ_K requires that $\phi_{L/K}$ be continuous for all L. Since $\mathrm{Gal}(L/K)$ is provided with the discrete topology, this implies that the kernel of $\phi_{L/K}$ is an open subgroup of $\mathbb{I}_K$, so that it contains a subgroup of the form

$$\prod_{v \in S} W_v \times \prod_{v \notin S} U_v\,,$$

where W_v are open subsets of $K_v^\times$ and S is a finite set of primes of K including the infinite primes. This fact, together with the previous observation, implies that $\phi_{L/K}(\alpha) = 1$ for those $\alpha \in \mathbb{I}_K$ whose components are all units and equal to 1 for infinite and ramified primes, and so determines $\phi_{L/K}$ for all $\alpha \in \mathbb{I}_K$. Therefore, since for all finite Abelian extension L the map $\phi_{L/K}$ is uniquely determined, so is ϕ_K. □

Definition 5.1.2. The *global Artin map* of a number field K is the map

$$\phi_K : \mathbb{I}_K \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$$

from the previous proposition.

The main theorems which we want to prove in this chapter are the Reciprocity Law and the Existence Theorem.

Theorem 5.1.3. (Reciprocity Law) Let K be a number field. Then, for all finite Abelian extension L/K, the map

$$\phi_{L/K} : \mathbb{I}_K \to \mathrm{Gal}(L/K)$$

is surjective with

$$\ker \phi_{L/K} = K^\times \cdot \mathrm{Nm}_{L/K}(\mathbb{I}_L)\,,$$

so that it induces an isomorphism

$$\phi_{L/K} : \mathbb{I}_K/(K^\times \cdot \mathrm{Nm}_{L/K}(\mathbb{I}_L)) \to \mathrm{Gal}(L/K)\,.$$

Note that the previous theorem obviously implies that $K^\times \subseteq \ker \phi_K$, so that we can define the Artin map on the idèle class group:

$$\phi_K : C_K \to \mathrm{Gal}(K^{\mathrm{ab}}/K)\,.$$

In this case, $\ker \phi_{L/K} = \mathrm{Nm}_{L/K} C_L$ and we get the isomorphism

$$\phi_{L/K} : C_K/\mathrm{Nm}_{L/K} C_L \to \mathrm{Gal}(L/K)\,.$$

Theorem 5.1.4. (Existence Theorem) Let K be a number field. Then, for any open subgroup N of C_K of finite index, there exists a unique (up to K-isomorphism) Abelian extension L of K such that $\mathrm{Nm}_{L/K} C_L = N$.

Observe that, because of the isomorphism

$$\phi_{L/K} : C_K/\mathrm{Nm}_{L/K} C_L \to \mathrm{Gal}(L/K)\,,$$

for all finite Abelian extension $\mathrm{Nm}_{L/K} C_L$ has finite index in C_K. We also know that $\mathrm{Nm}_{L/K} C_L$ is open because of Proposition 4.2.4. Therefore, these two theorems provide a bijection between the Abelian extensions of K and the open subgroups of finite index of C_K.

5.2 The cohomology of the units

References: [Mil13], [Neu99]

We begin this section with some technical lemmas.

Lemma 5.2.1. Let G be a finite group and let k be an infinite field. Let M and N be $k[G]$-modules which are of finite dimension as k-vector spaces. Let $\Omega \supseteq k$ be a field. Then, if $M \otimes_k \Omega$ and $N \otimes_k \Omega$ are isomorphic as $\Omega[G]$-modules, M and N are isomorphic as $k[G]$-modules.

Proof. Since both M and N are finite dimesional k-vector spaces, choose a basis for each of them. For each $\sigma \in G$, the maps

$$\begin{array}{ll} M \to M & N \to N \\ m \mapsto \sigma m & n \mapsto \sigma n \end{array}$$

are both k-linear, so that, in the chosen bases, they are given by matrices which we will denote respectively by $B(\sigma)$ and $C(\sigma)$. A $k[G]$-homomorphism from M to N is a k-linear map ϕ satisfying $\phi(\sigma m) = \sigma\phi(m)$ for all $\sigma \in G$ and all $m \in M$, i.e it is a map that in the chosen bases is given by a matrix A satisfying

$$AB(\sigma) = C(\sigma)A$$

for all $\sigma \in G$. We have, then, a finite set of linear conditions on the coefficients of A.

If $v_1, \ldots, v_n$ is a basis of M as a k-vector space, $v_1 \otimes_k 1, \ldots, v_n \otimes_k 1$ is a basis of $M \otimes_k \Omega$ as a Ω-vector space, and the same for N, so that we can choose as Ω-bases of $M \otimes_k \Omega$ and $N \otimes_k \Omega$ the bases obtained from the previously chosen k-bases of M and N in this way, and, with these bases, the condition for a k-linear map being a $\Omega[G]$-homomorphism, in terms of the associated matrix, is the same, i.e. a map $M \otimes_k \Omega \to N \otimes_k \Omega$ is a $\Omega[G]$-homomorphism if and only if it is given by a matrix A satisfying

$$AB(\sigma) = C(\sigma)A$$

for all $\sigma \in G$.

Since $\dim_k M = \dim_\Omega M \otimes_k \Omega$ and $\dim_k N = \dim_\Omega N \otimes_k \Omega$, we get:

$$\dim_k \mathcal{L}(M, N) = \dim_\Omega \mathcal{L}(M \otimes_k \Omega, N \otimes_k \Omega)\,,$$

and, since the condition for a k-linear map in $\mathcal{L}(M, N)$ being a $k[G]$-homomorphism and the condition for a Ω-linear map in $\mathcal{L}(M \otimes_k \Omega, N \otimes_k \Omega)$ being a $\Omega[G]$-homomorphism are given by the same system of linear equations, we get

$$\dim_k \mathrm{Hom}_{k[G]}(M, N) = \dim_\Omega \mathrm{Hom}_{\Omega[G]}(M \otimes_k \Omega, N \otimes_k \Omega)\,,$$

and, if $\phi_1, \ldots, \phi_r$ form a basis of $\mathrm{Hom}_{k[G]}(M, N)$, then they also form a basis of the vector subspace $\mathrm{Hom}_{\Omega[G]}(M \otimes_k \Omega, N \otimes_k \Omega)$ when extended naturally.

Define

$$p(X_1, \ldots, X_r) = \det(X_1\phi_1 + \cdots + X_r\phi_r)\,.$$

Since $\phi_1, \ldots, \phi_r$ are given by matrices with coefficients in k, $p(X_1, \ldots, X_r) \in k[X_1, \ldots, X_r]$. The fact that $M \otimes_k \Omega$ and $N \otimes_k \Omega$ are isomorphic as $\Omega[G]$-modules means that there is an $\Omega[G]$-isomorphism

$$\phi : M \otimes_k \Omega \to N \otimes_k \Omega\,.$$

Since $\phi \in \mathrm{Hom}_{\Omega[G]}(M \otimes_k \Omega, N \otimes_k \Omega)$, there exist $\alpha_1, \ldots, \alpha_r \in \Omega$ such that

$$\phi = \alpha_1\phi_1 + \cdots + \alpha_r\phi_r\,,$$

and the fact that ϕ is an isomorphism implies

$$p(\alpha_1, \ldots, \alpha_r) \neq 0\,,$$

so that $p(X_1, \ldots, X_r)$ is not the null polynomial. But, since k is infinite, this implies that there exist $a_1, \ldots, a_r \in k$ such that

$$p(a_1, \ldots, a_r) \neq 0\,,$$

and so there exists a $k[G]$-isomorphism

$$a_1\phi_1 + \cdots + a_r\phi_r : M \to N\,.$$

□

Lemma 5.2.2. Let G be a finite cyclic group and let M and N be G-modules which are finitely generated as Abelian groups (i.e. as $\mathbb{Z}$-modules). Suppose that $M \otimes_{\mathbb{Z}} \mathbb{Q}$ and $N \otimes_{\mathbb{Z}} \mathbb{Q}$ are isomorphic as G-modules. Then, if either $h(M)$ or $h(N)$ is defined, so is the other and they are equal.

Proof. By Proposition 1.9.11, we may assume that both M and N are torsion free, so that, as Abelian groups, $M \simeq \mathbb{Z}^r$ and $N \simeq \mathbb{Z}^s$ for some integers $r, s \geqslant 1$. Since $M \otimes_{\mathbb{Z}} \mathbb{Q}$ and $N \otimes_{\mathbb{Z}} \mathbb{Q}$ are isomorphic as G-modules, so they are as Abelian groups, so that

$$\mathbb{Q}^r \simeq M \otimes_{\mathbb{Z}} \mathbb{Q} \simeq N \otimes_{\mathbb{Z}} \mathbb{Q} \simeq \mathbb{Q}^s \,,$$

whereby we deduce $r = s$.

Let $m_1, \ldots, m_r$ be a basis of M as a free $\mathbb{Z}$-module. Then, $m_1 \otimes_{\mathbb{Z}} 1, \ldots m_r \otimes_{\mathbb{Z}} 1$ is a basis of $M \otimes_{\mathbb{Z}} \mathbb{Q}$ as a $\mathbb{Q}$-vector space. Let

$$\phi : M \otimes_{\mathbb{Z}} \mathbb{Q} \to N \otimes_{\mathbb{Z}} \mathbb{Q}$$

be a homomorphism of G-modules. Then, it is also an isomorphism of $\mathbb{Q}$-vector spaces, so that the elements $\phi(m_1 \otimes_{\mathbb{Z}} 1), \ldots, \phi(m_r \otimes_{\mathbb{Z}} 1)$ form a basis of $N \otimes_{\mathbb{Z}} \mathbb{Q}$. Let $n_1, \ldots, n_r$ be a basis of N as a $\mathbb{Z}$-module. Multiplying ϕ by a suitable $d \in \mathbb{Z}$, we may assume that all $\phi(m_i \otimes_{\mathbb{Z}} 1)$ belong to the $\mathbb{Z}$-submodule of $N \otimes_{\mathbb{Z}} \mathbb{Q}$ generated by $n_1 \otimes_{\mathbb{Z}} 1, \ldots, n_r \otimes_{\mathbb{Z}} 1$, which can be naturally identified with N. The $\mathbb{Z}$-submodule of $M \otimes_{\mathbb{Z}} \mathbb{Q}$ generated by $m_1 \otimes_{\mathbb{Z}} 1, \ldots m_r \otimes_{\mathbb{Z}} 1$ can also be naturally identified with M. With these identifications, we get that $\phi(M) \subseteq N$ is a full latice in $N \otimes_{\mathbb{Z}} \mathbb{Q}$, so that $\phi(M)$ has finite index in N and ϕ is clearly injective. Then, by Corollary 1.9.12, we deduce that, whenever $h(M)$ or $h(N)$ is defined, both are and $h(M) = h(N)$. □

Lemma 5.2.3. Let G be a finite cyclic group and let V be a finite-dimensional real vector space on which G acts linealy. Let M and N be full latices of V which are stable under the action of G. Then, if either $h(M)$ or $h(N)$ is defined, so is the other and they are equal.

Proof. Since both M and N are full latices in V and the action of G on V is $\mathbb{R}$-lineal, the canonical maps

$$\begin{aligned} M \otimes_{\mathbb{Z}} \mathbb{R} &\to V & N \otimes_{\mathbb{Z}} \mathbb{R} &\to V \\ \sum_i m_i \otimes_{\mathbb{Z}} x_i &\mapsto \sum_i x_i m_i & \sum_i n_i \otimes_{\mathbb{Z}} x_i &\mapsto \sum_i x_i n_i \end{aligned}$$

are G-isomorphisms, so that, by Lemma 5.2.1, $M \otimes_{\mathbb{Z}} \mathbb{Q}$ and $N \otimes_{\mathbb{Z}} \mathbb{Q}$ are isomorphic as G-modules. Then, by the previous lemma, we get the desired result. □

Proposition 5.2.4. Let S be a finite set of primes of K containing all infinite primes, and let $s = |S|$. Define

$$U(S) = \{\alpha \in K : \mathrm{ord}_v(\alpha) = 0 \text{ for all } v \notin S\} \,.$$

Then, the homomorphism

$$\begin{aligned} \lambda : U(S) &\to \prod_{v \in S} \mathbb{R} \\ a &\mapsto (\log |a|_v)_{v \in S} \end{aligned}$$

has kernel $\mu(K)$ (i.e. the roots of unity in K) and its image is a full latice in the $(s-1)$-dimensional real vector space

$$H = \left\{ (x_v)_{v \in S} : \sum_{v \in S} x_v = 0 \right\} .$$

Proof. Let S_∞ be the set of all infinite primes of K, and let $S_f = S \setminus S_\infty$. When $S = S_\infty$, the proposition is simply Dirichlet's unit theorem. For the general case, let J be the subgroup of I_K generated by the primes in S_f, let $t = |J|$, and consider the diagram

$$\begin{array}{ccccc} 0 & \longrightarrow & \mathcal{O}_K^\times & \longrightarrow & U(S) & \xrightarrow{a \mapsto (a)} & J \\ & & \downarrow{\scriptstyle \lambda'} & & \downarrow{\scriptstyle \lambda} & & \downarrow{\scriptstyle \lambda''} \\ 0 & \longrightarrow & \prod_{v\in S_\infty} \mathbb{R} & \longrightarrow & \prod_{v\in S} \mathbb{R} & \longrightarrow & \prod_{v\in S_f} \mathbb{R} \end{array},$$

where λ' is the map corresponding to Dirichlet's unit theorem and λ'' is the map defined by

$$\prod_{v\in S_f} \mathfrak{p}_v^{m_v} \mapsto (-m_v \log(\mathrm{Nm}(\mathfrak{p}_v)))_{v\in S_f}$$

(recall that $|a|_v = \mathrm{Nm}(\mathfrak{p}_v)^{-\mathrm{ord}_v(a)}$). It is obvious that the diagram commutes and that the rows are exact. Moreover, it is clear that λ'' maps J isomorphically to the lattice spanned by the vectors $(0,\dots,0,\mathrm{Nm}(\mathfrak{p}),0\dots,0)$ with $\mathfrak{p} \in S_f$. In particular, since λ'' is injective, we deduce that $\ker\lambda = \ker\lambda' = \mu(K)$.

On the other hand, again taking into account hat λ'' is injective, we easily deduce that the sequence

$$0 \longrightarrow \mathrm{Im}\,\lambda' \longrightarrow \mathrm{Im}\,\lambda \longrightarrow \mathrm{Im}\,\lambda''\,,$$

is exact. Since both $\mathrm{Im}\,\lambda'$ and $\mathrm{Im}\,\lambda''$ are lattices, so is $\mathrm{Im}\,\lambda$. Let $i(U(S))$ be the image of $U(S)$ in J under the map $a \mapsto (a)$. If h is the class number of K, then clearly $J^h \subseteq i(U(S)) \subseteq J$, which shows that $i(U(S))$ has rank t. Then, the image of $\mathrm{Im}\,\lambda$ under the last arrow in the previous exact sequence has rank t; the kernel of this arrow, which is $\mathrm{Im}\,\lambda'$, has rank $|S_\infty| - 1 = s - t - 1$, and, consequently, the lattice $\mathrm{Im}\,\lambda'$ has rank $t + s - t - 1 = s - 1$ and lies in H because of the product formula (Proposition 2.6.2). □

Proposition 5.2.5. Let L/K be a finite cyclic extension of number fields with Galois group $G = \mathrm{Gal}(L/K)$. Let S be a finite set of primes of K containing all infinite primes. Let T be the set of primes of L lying above any prime of S. Define

$$U(T) = \{\alpha \in L : \mathrm{ord}_w(\alpha) = 0 \text{ for all } w \notin T\}\,.$$

Then

$$n \cdot h(G, U(T)) = \prod_{v\in S} n_v\,,$$

where $n = [L:K]$ and $n_v = [L^v : K_v]$.

Proof. Let $V = \mathrm{Hom}(T, \mathbb{R})$. Define an action of G on V by

$$(\sigma f)(w) = f(\sigma^{-1} w) \text{ for all } \sigma \in G, w \in T\,.$$

Let $N = \mathrm{Hom}(T, \mathbb{Z})$. Then, N is a full latice of the finite-dimensional real vector space V which is stable under the action of G. Since, for all $v \in S$, G acts transitively on the set of primes $w|v$, there is a bijection

$$G/G^v \to \{w \in \mathrm{Spec}(\mathcal{O}_L) : w|v\}$$

and we get:

$$\mathrm{Hom}(T,\mathbb{Z}) \simeq \bigoplus_v \mathrm{Hom}(G/G^v,\mathbb{Z})$$

(as G-modules). It is straightforward that the map

$$\begin{aligned}\mathrm{Hom}(G/G^v,\mathbb{Z}) &\to \mathrm{Ind}_{G^v}^G(\mathbb{Z})\\ \phi &\mapsto \tilde{\phi}\end{aligned}$$

defined by $\tilde{\phi}(\sigma) = \phi([\sigma^{-1}])$ for all $\sigma \in G$ is a G-isomorphism. Then, we get

$$h(G,N) = \prod_{v\in S} h(G,\mathrm{Ind}_{G^v}^G(\mathbb{Z})) = \prod_{v\in S} h(G^v,\mathbb{Z}) = \prod_{v\in S} |G^v| = \prod_{v\in S} n_v\,,$$

where, in the second equality, we have used Shapiro's lemma.

By the previous proposition, the homomorphism

$$\begin{aligned}\lambda : U(T) &\to \prod_{w\in T} \mathbb{R} \simeq V\\ a &\mapsto (\log|a|_w)_{w\in T}\end{aligned}$$

has kernel $\mu(L)$ and its image, which we will denote my M^0, is a full latice in

$$H = \left\{ (x_w)_{w\in T} : \sum_{w\in T} x_w = 0 \right\}.$$

The map $\lambda : U(T) \to V$ commutes with the action of G, so that it is a G-homomorphism and M^0 is stable under the action of G. Since $\mu(L)$ is finite, we know, by Corollary 1.9.12, that $h(U(T)) = h(M^0)$, provided that one of these two Herbrand quotients exists. The vector $e = (1,\dots 1) \in V$ is clearly stable under the action of G. Let $M = M^0 \oplus \mathbb{Z}e$. Then, M is clearly a full latice in V which is stable under the action of G, so that, by Lemma 5.2.3, $h(M) = h(N)$. Moreover,

$$h(G,M) = h(G,M^0)h(G,\mathbb{Z}e) = h(G,U(T))|G| = n\cdot h(G,U(T))$$

and we get the desired result. □

5.3 The first inequality

References: [Mil13]

Proposition 5.3.1. Let L/K be a finite Galois extension of number fields with Galois group $G = \mathrm{Gal}(L/K)$. Then, the canonical map $C_K \to C_L$ induces an isomorphism

$$C_K \to C_L^G = H^0(G,C_L)\,.$$

Proof. The short exact sequence of G-modules

$$0 \to L^\times \to \mathbb{I}_L \to C_L \to 0$$

gives rise to the long cohomology sequence

$$0 \to H^0(G, L^\times) \to H^0(G, \mathbb{I}_L) \to H^0(G, C_L) \to H^1(G, L^\times) \to \cdots .$$

By Hilbert's theorem 90 we have $H^1(G, L^\times) = 0$, so that we get the short exact sequence

$$0 \to L^{\times G} \to \mathbb{I}_L^G \to C_L^G \to 0 .$$

Then, we get the commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & K^\times & \longrightarrow & \mathbb{I}_K & \longrightarrow & C_K & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & L^{\times G} & \longrightarrow & \mathbb{I}_L^G & \longrightarrow & C_L^G & \longrightarrow & 0 \end{array}$$

where the rows are exact and the vertical arrows are the natural inclusions (the fact that the image of C_K in C_L under the canonical inclusions lies in C_L^G can be checked directly or deduced from the same diagram). Since the first two vertical arrows are isomorphisms (the first one is clear and for the second one see Proposition 4.3.6) so is the third, which proves the proposition. □

Theorem 5.3.2. Let L/K be a finite cyclic extension of number fields. Then,

$$h(G, C_L) = [L : K] .$$

Proof. Let S be a set of primes of K containing all infinite primes, all finite primes that ramify in L, and the finite primes lying under a finite set of primes of L generating Cl_L.

By Lemma 4.1.4,

$$\mathbb{I}_L = \mathbb{I}_L^S L^\times ,$$

so that we get

$$C_L = \mathbb{I}_L/L^\times = \mathbb{I}_L^S L^\times / L^\times \simeq \mathbb{I}_L^S / \mathbb{I}_L^S \cap L^\times .$$

Note that $\mathbb{I}_L^S \cap L^\times = U(T)$, where T is the set of primes of L lying above some prime in S. Then, we get a short exact sequence

$$0 \to U(T) \to \mathbb{I}_L^S \to C_L \to 0 ,$$

from which we deduce

$$h(G, \mathbb{I}_L^S) = h(G, U(T)) \cdot h(G, C_L)$$

and the theorem is then a consequence of Proposition 4.3.8 and Proposition 5.2.5. □

Corollary 5.3.3. (First inequality) Let L/K be a finite cyclic extension of number fields. Then,

$$[\mathbb{I}_K : K^\times \cdot \mathrm{Nm}_{L/K} \mathbb{I}_L] \geqslant [L : K] .$$

Proof. By Proposition 4.2.3,

$$[\mathbb{I}_K : K^\times \cdot \mathrm{Nm}_{L/K} \mathbb{I}_L] = [C_K : \mathrm{Nm}_{L/K} C_L] .$$

On the other hand,

$$h(G, C_L) = \frac{|H^0_T(G, C_L)|}{|H^1(G, C_L)|} = \frac{[C^G_L : \mathrm{Nm}_{L/K} C_L]}{|H^1(G, C_L)|} = \frac{[C_K : \mathrm{Nm}_{L/K} C_L]}{|H^1(G, C_L)|}$$

and, from the previous theorem, we deduce

$$[C_K : \mathrm{Nm}_{L/K} C_L] \geqslant [L : K] \,,$$

whereby the desired inequality follows. □

Lemma 5.3.4. Let L/K be a finite solvable extension of number fields. If there exists a subgroup $D \subseteq \mathbb{I}_K$ such that $D \subseteq \mathrm{Nm}_{L/K} \mathbb{I}_L$ and $K^\times D$ is dense in $\mathbb{I}_K$, then $L = K$.

Proof. If $L \neq K$, there exists a field $K' \neq K$ such that K'/K is a non-trivial cyclic extension.

We have

$$D \subseteq \mathrm{Nm}_{L/K} \mathbb{I}_L = \mathrm{Nm}_{K'/K}(\mathrm{Nm}_{L/K'} \mathbb{I}_L) \subseteq \mathrm{Nm}_{K'/K} \mathbb{I}_{K'} \,.$$

Since $K^\times D$ is dense in $\mathbb{I}_K$, so also is $K^\times \mathrm{Nm}_{K'/K} \mathbb{I}_{K'}$. Then, since $K^\times \mathrm{Nm}_{K'/K} \mathbb{I}_{K'}$ is an open subgroup of $\mathbb{I}_K$ by Proposition 4.2.4, we get

$$K^\times \mathrm{Nm}_{K'/K} \mathbb{I}_{K'} = \mathbb{I}_K \,,$$

as, otherwise, for $\alpha \in \mathbb{I}_K \setminus K^\times \mathrm{Nm}_{K'/K} \mathbb{I}_{K'}$, $\alpha K^\times \mathrm{Nm}_{K'/K} \mathbb{I}_{K'}$ would be an open neighborhood of α disjoint with $K^\times \mathrm{Nm}_{K'/K} \mathbb{I}_{K'}$, contradicting the fact that this set is dense.

Finally, the first inequality gives us

$$1 = [\mathbb{I}_K : K^\times \cdot \mathrm{Nm}_{K'/K} \mathbb{I}_{K'}] \geqslant [K' : K] \,,$$

which contradicts the assumption $K' \neq K$. □

Proposition 5.3.5. Let L/K be a finite solvable extension of number fields. If $L \neq K$, there are infinitely many primes of K that do not split completely in L.

Proof. Assume that there are only finitely many primes of K that do not split completely in L. Let S be a finite set of primes of K containing all infinite primes and the finite primes that do not split completely. Define

$$U^S_K = \{\alpha \in \mathbb{I}_K : \alpha_v = 1 \text{ for all } v \in S\} \,.$$

Observe that U^S_K is clearly a subgroup of $\mathbb{I}_K$. Since S contains all primes which do not split completely, we have $L_w = K_v$ for all $v \notin S$ and all $w|v$. For $\alpha = (\alpha_v)_v \in U^S_K$, choose some prime $w_v|v$ of L for each prime $v \notin S$ of K, define $\beta_{w_v} = \alpha_v$ for each $v \notin S$ and $\beta_w = 1$ for all other primes w of L, and let $\beta = (\beta_w)_w \in \mathbb{I}_L$. Then, $\alpha = \mathrm{Nm}_{L/K} \beta$. Therefore, we see that $U^S_K \subseteq \mathrm{Nm}_{L/K} \mathbb{I}_L$.

Now, let $\alpha = (\alpha_v)_v \in \mathbb{I}_K$. By the weak approximation theorem, we can choose $a \in K^\times$ which is arbitrarily close to each of the α_v with $v \in S$ in the corresponding valued field K_v. Take $\alpha' = (\alpha'_v)_v$ with $\alpha'_v = 1$ for all $v \in S$ and $\alpha'_v = a^{-1}\alpha_v$ for all $v \notin S$. Then, $\alpha' \in U^S_K$. In this way, we can find an element $a\alpha' \in K^\times U^S_K$ which is arbitrarily close to α. Hence, we see that $K^\times U^S_K$ is dense in $\mathbb{I}_K$.

Since U^S_K satisfies the hypothesis of the previous lemma, we deduce that $L = K$. □

Proposition 5.3.6. Let L/K be a finite solvable extension with Galois group $G = \mathrm{Gal}(L/K)$. Then, for every finite set T of primes of L containing all infinite primes and all finite primes above some prime of K which ramifies in L, the Fröbenius automorphisms $(\mathfrak{P}, L/K)$ with $\mathfrak{P} \notin T$ generate G.

Proof. Let H be the subgroup of G generated by the Fröbenius automorphisms $(\mathfrak{P}, L/K)$ with $\mathfrak{P} \notin T$. Let $E = L^H$. Since E is the subfield of L fixed by H, all the Fröbenius automorphisms $(\mathfrak{P}, L/K)$ with $\mathfrak{P} \notin T$ act as the identity map on E. Consequently, taking into account the identity

$$(\mathfrak{P} \cap E, E/K) = (\mathfrak{P}, L/K)|_E = \mathrm{id}_E\,,$$

we deduce that all finite primes of E which are of the form $\mathfrak{P} \cap E$ for some $\mathfrak{P} \notin T$ have trivial decomposition group over K. This means that all finite primes of K which are under a prime $\mathfrak{P} \notin T$ split completely in E. Since this accounts for all but finitely many primes of K, from the last proposition we deduce that $K = E$, and consequently $H = G$. □

Corollary 5.3.7. Let L/K be a finite Abelian extension of number fields with Galois group $G = \mathrm{Gal}(L/K)$. Then, for every finite set S of primes of K including all infinite primes and the primes which ramify in L, the Fröbenius automorphisms $(\mathfrak{p}, L/K)$ with $\mathfrak{p} \notin S$ generate G.

5.4 The second inequality

References: [Mil13]

Our aim in this section is to prove the following theorem.

Theorem 5.4.1. Let L/K be a finite Galois extension of number fields with Galois group $G = \mathrm{Gal}(L/K)$. Then:

1. $[\mathbb{I}_K : K^\times \cdot \mathrm{Nm}_{L/K}\mathbb{I}_L]$ is finite and divides $[L : K]$.
2. $H^1(G, C_L) = 0$.
3. $H^2(G, C_L)$ is finite of order a divisor of $[L : K]$.

We will prove this theorem in a series of steps.

Lemma 5.4.2. It is enough to prove Theorem 5.4.1 in the case in which G is a p-group for some prime p.

Proof. Assume that the theorem holds in this case, and let L/K be as in the statement of the theorem, with Galois group G. Let p be any prime, and let H be a p-Sylow subgroup of G. Then, by Corollary 1.4.5, the restriction map

$$\mathrm{Res} : H^r_T(G, C_L) \to H^r_T(H, C_L)$$

is injective when restricted to the p-primary component of $H^r_T(G, C_L)$.

Also note that

$$H^0_T(G, C_L) \simeq C_L/\mathrm{Nm}_{L/K}C_L \simeq \mathbb{I}_L/\left(K^\times \cdot \mathrm{Nm}_{L/K}\mathbb{I}_L\right)\,.$$

Since H is the Galois group of L/L^H, then, by assumption, the theorem holds for this extension. Hence, the orders of $H^0_T(H, C_L)$ and $H^2(H, C_L)$ are finite and divisors of $[L : L^H]$

(i.e they are powers of p dividing $[L:K]$) and $H^1(G,C_L)=0$. Consequently, by the injectivity of the previous restriction map on the corresponding p-primary components, we know that the p-primary components of $H^0_T(G,C_L)$ and $H^2(G,C_L)$ are powers of p dividing $[L:K]$, whereas the p-primary component of $H^1(G,C_L)$ is trivial. Since this holds for all prime p, we see that the theorem also holds for L/K. □

Lemma 5.4.3. It is enough to prove Theorem 5.4.1 in the case in which G is a cyclic group of prime order p.

Proof. Assume that the theorem holds in this case. We will show that then it also holds when G is a p-group, which, by the previous lemma, implies the general case. We will argue by induction on the order of the Galois group of the extension. If the extension is trivial, the theorem follows easily. Now, let L/K be a non-trivial extension having as Galois group a p-group G, and assume that we already know that the theorem holds for the case of p-groups of order less than G. Since G is a p-group, it has a normal subgroup H of index p. Consider the inflation-restriction exact sequence

$$0 \to H^1(G/H, C_L^H) \to H^1(G,C_L) \to H^1(H,C_L)\,.$$

By induction, $H^1(H,C_L)=0$. On the other hand, it is easy to see that the isomorphism $C_{L^H} \simeq C_L^H$ from Proposition 5.3.1 is in this case a G/H-isomorphism, so that we get an isomorphism $H^1(G/H,C_L^H) \simeq H^1(G/H,C_{L^H})$, where the second group is trivial by assumption, as G/H is the Galois group of L^H/K, which is cyclic of order p. Then, from the exact sequence we deduce $H^1(G,C_L)=0$. Since $H^1(H,C_L)=0$, we also have the inflation-restriction exact sequence

$$0 \to H^2(G/H, C_{L^H}) \to H^2(G,C_L) \to H^2(H,C_L)\,.$$

By induction, $H^2(H,C_L)$ is finite and has order a divisor of $[L:L^H]$, and, by assumption, $H^2(G/H,C_{L^H})$ is also finite and a divisor of $[L^H:K]=p$. Then, by the previous exact sequence, we know that $|H^2(G,C_L)|$ is a divisor of $|H^2(G/H,C_{L^H})|\cdot|H^2(H,C_L)|$ and so a divisor of $[L:K]$.

For the first statement of the theorem, observe that

$$[C_K : \mathrm{Nm}_{L/K}C_L] = [C_K : \mathrm{Nm}_{L^H/K}C_{L^H}]\cdot[\mathrm{Nm}_{L^H/K}C_{L^H} : \mathrm{Nm}_{L/K}C_L]\,.$$

Here, $[C_K : \mathrm{Nm}_{L^H/K}C_{L^H}]$ divides $[L^H:K]=p$ by assumption. Also, we have the surjective homomorphism

$$\mathrm{Nm}_{L^H/K} : C_{L^H}/\mathrm{Nm}_{L/L^H}C_L \to \mathrm{Nm}_{L^H/K}C_{L^H}/\mathrm{Nm}_{L/K}C_L\,,$$

from which we deduce that $[\mathrm{Nm}_{L^H/K}C_{L^H} : \mathrm{Nm}_{L/L^H}C_L]$ divides $[C_{L^H} : \mathrm{Nm}_{L^H/K}C_{L^H}]$, which, in turn, divides $[L:L^H]$ by induction. Then, we deduce that $[C_K : \mathrm{Nm}_{L/K}C_L]$ divides $[L:K]$. □

Lemma 5.4.4. Under the assumptions of Theorem 5.4.1, if G is cyclic, the three statements of the theorem are equivalent.

Proof. The equivalence of statements 1 and 3 is immediate taking into account that, for a finite cyclic group G and any G-module M, the corresponding Tate cohomology groups are 2-periodic, i.e.

$$H^r_T(G,M) \simeq H^{r+2}_T(G,M)$$

for all $r \in \mathbb{Z}$ (see Proposition 1.9.8).

By Theorem 5.3.2, $h(G,C_L)=[L:K]$. Then, since

$$h(G,C_L) = \frac{|H^0_T(G,C_L)|}{|H^1(G,C_L)|} = \frac{|H^2(G,C_L)|}{|H^1(G,C_L)|}$$

the equivalence between statement 2 and the other two statements follows easily (in fact, we see that necessarily $[C_K : \mathrm{Nm}_{L/K} C_L] = |H^2(G, C_L)| = [L : K]$). □

Then, summarizing the previous results, it suffices to prove Theorem 5.4.1 for the case in which G is cyclic of prime order p and, moreover, it is enough to prove one of the three statements in the theorem for this particular case. We will then focus on proving the first statement of the theorem, which is often referred to as the *second inequality*.

Lemma 5.4.5. It is enough to prove the second inequality in the case in which G is a cyclic group of prime order p and K contains a primitive p-th root of unity.

Proof. By the previous results, we need only see that if the second inequality holds in this case then it also holds whenever G is a cyclic group of prime order p.

Then, let L/K be a finite Galois extension of number fields with cyclic Galois group of prime order p. Let Ω be an algebraic closure of L (and K), and let $\zeta \in \Omega$ be a primitive p-root of unity. Let $K' = K(\zeta)$ and $L' = L(\zeta)$. All these extensions are clearly Galois over K. Observe that $[K' : K] = [K(\zeta) : K] \leqslant [\mathbb{Q}(\zeta) : \mathbb{Q}] = p - 1$, so that $[K' : K]$ is relatively prime to $[L : K] = p$ and, consequently, $K' \cap L = K$. Then, the map

$$\begin{aligned} \mathrm{Gal}(L'/K') &\to \mathrm{Gal}(L/K) \\ \sigma &\mapsto \sigma|_L \end{aligned}$$

is an isomorphism.

Consider the following diagram:

$$\begin{array}{ccccccc}
C_L & \xrightarrow{\mathrm{Nm}_{L/K}} & C_K & \longrightarrow & C_K/\mathrm{Nm}_{L/K} C_L & \longrightarrow & 0 \\
\downarrow{\scriptstyle i_L} & & \downarrow{\scriptstyle i_K} & & \downarrow & & \\
C_{L'} & \xrightarrow{\mathrm{Nm}_{L'/K'}} & C_{K'} & \longrightarrow & C_{K'}/\mathrm{Nm}_{L'/K'} C_{L'} & \longrightarrow & 0 \\
\downarrow{\scriptstyle \mathrm{Nm}_{L'/L}} & & \downarrow{\scriptstyle \mathrm{Nm}_{K'/K}} & & \downarrow & & \\
C_L & \xrightarrow{\mathrm{Nm}_{L/K}} & C_K & \longrightarrow & C_K/\mathrm{Nm}_{L/K} C_L & \longrightarrow & 0
\end{array}$$

Its rows are obviuosly exact. We claim that the two squares in the left form a commutative diagram (this allows us to define the vertical arrows in the right, and the whole diagram is then commutative). To prove it, consider, first, the upper left square. Take any element in C_L; let it be the class of $(\alpha_v)_v$, where v runs through the primes of L. If we go down in the diagram, we obtain the class of $(\beta_w)_w$, where w runs through the primes of L' and $\beta_w = \alpha_v$ if $w|v$. Now, going right, we obtain the class of $(\gamma_u)_u$, with

$$\gamma_u = \prod_{\sigma \in \mathrm{Gal}(L'/K')} \sigma\beta_{\sigma^{-1}w} = \prod_{\sigma \in \mathrm{Gal}(L'/K')} \sigma\alpha_{(\sigma^{-1}|_L)(v)} = \prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma\alpha_{\sigma^{-1}v}\,,$$

where w is any prime of L' dividing u and v the prime of L under w. Since w divides both u and v, u and v lie over the same prime of K, and so we can say that

$$\gamma_u = \prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma\alpha_{\sigma^{-1}v}$$

for any prime v of L lying over the same prime of K as u. This is easily the same that we obtain if we go first right and then down in the diagram.

The square down left is easily commutative because

$$\mathrm{Nm}_{L/K} \circ \mathrm{Nm}_{L'/L} = \mathrm{Nm}_{L/K} = \mathrm{Nm}_{K'/K} \circ \mathrm{Nm}_{L'/K'} .$$

Now, we claim that the maps $\mathrm{Nm}_{L'/L} \circ i_L$ and $\mathrm{Nm}_{K'/K} \circ i_K$ are both multiplication by $m = [L' : L] = [K' : K]$. We prove it for $\mathrm{Nm}_{L'/L} \circ i_L$; the other case is obviously analogous. Take any element in C_L; let it be the class of the idèle $(\alpha_v)_v$, where v runs through the primes of L. Then, i_L maps it to the class of the idèle $(\beta_w)_w$, with w running through the primes of L' and $\beta_w = \alpha_v$ if $w|v$. Applying the norm map, we get the class of the idèle $(\gamma_v)_v$, where, if w is any prime of L' dividing v,

$$\gamma_v = \prod_{\sigma \in \mathrm{Gal}(L'/L)} \sigma\beta_{\sigma^{-1}w} = \prod_{\sigma \in \mathrm{Gal}(L'/L)} \sigma\alpha_v = \alpha_v^m .$$

The composite of the vertical arrows at the right of the diagram is hence multiplication by m, too. But, since all the elements in $C_K/\mathrm{Nm}_{L/K}C_L$ have order a divisor of $[L : K] = p$ (because the composite of the inclusion $C_K \to C_L$ and the norm map $\mathrm{Nm}_{L/K}$ is multiplication by p), multiplication by m is an isomorphism. In particular, we deduce that the homomorphism

$$C_{K'}/\mathrm{Nm}_{L'/K'}C_{L'} \to C_K/\mathrm{Nm}_{L/K}C_L$$

is surjective, so that $[C_K : \mathrm{Nm}_{L/K}C_L]$ divides $[C_{K'} : \mathrm{Nm}_{L'/K'}C_{L'}]$, which, by assumption, divides $[L' : K'] = [L : K]$. □

We have reduced the proof of Theorem 5.4.1 to proving the second inequality for the case in which G is cyclic of prime order p and K contains a p-th root of unity. We will now give a proof of the second inequality which is valid in a slightly more general case: allowing G to be any finite Abelian group of exponent p.

Let L/K be a finite Abelian extension of number fields with Galois group $G = \mathrm{Gal}(L/K)$. Assume that G has prime exponent p, and K contains a primitive p-th root of unity ζ. Then, if $[L : K] = p^r$,

$$G \simeq (\mathbb{Z}/p\mathbb{Z})^r .$$

By Proposition A.0.4, we know that such an extension can be obtained adjoining p-th roots of elements of K. Taking this into account, as well as the fact that, by Proposition A.0.1, when we adjoin a p-th root the degree of the extension is either 1 or p, we get that

$$L = K(a_1^{1/p}, \ldots, a_r^{1/p})$$

for some $a_i \in K^\times$, $i = 1, \ldots, r$. We may assume that $a_i \in \mathcal{O}_K$ for all i.

Let S be a finite set of primes of K containing all infinite primes, all primes dividing p or any of the a_i, and a finite set of generators of Cl_K. As previously, define

$$U(S) = \{a \in K : |a|_v = 1 \text{ for all } v \notin S\}$$

By Proposition 5.2.4, it follows that

$$U(S) \simeq \mu(K) \times \mathbb{Z}^{s-1}$$

where $s = |S|$. Observe that $\mu(K)$ is cyclic since it is a finite subgroup of $K^\times$, and it has order divisible by p since K contains a primitive p-th root of unit. Then, from the previous isomorphism, we get

$$U(S)/U(S)^p \simeq (\mathbb{Z}/p\mathbb{Z})^s$$

Define $M = K(U(S)^{1/p}) = K(U(S) \cdot K^{\times p}/K^{\times p})$. Observe that

$$U(S) \cdot K^{\times p}/K^{\times p} \simeq U(S)/U(S) \cap K^{\times p} = U(S)/U(S)^p \simeq (\mathbb{Z}/p\mathbb{Z})^s$$

Then, M is the Abelian extension of exponent p corresponding to the finite subgroup of $K^\times/K^{\times p}$ given by $U(S) \cdot K^{\times p}/K^{\times p}$ (see Proposition A.0.4). Therefore,

$$K^\times \cap M^{\times p} = U(S) \cdot K^{\times p}$$

and, by Lemma A.0.3, we have $[M : K] = |\mathrm{Gal}(M/K)| = p^s$.

Since S contains all finite primes dividing any of the a_i, we have $a_i \in U(S)$ for all i and so $L \subseteq M$. Let $t = s - r$, so that $[M : L] = p^t$.

Lemma 5.4.6. With the previous definitions and assumptions, there exists a finite set T of primes of K, disjoint from S, such that the Fröbenius elements $(\mathfrak{p}_v, M/K)$ with $v \in T$ form a basis of $\mathrm{Gal}(M/L)$ as a $\mathbb{F}_p$-vector space.

Proof. First, note that the only primes dividing either p or any element in $U(S)$ are those contained in S, so that, by Proposition A.0.5, the set S contains all the primes of K that ramify in M. Therefore, for any prime of K $u \notin S$ and any prime $w|u$ of M, the extension M_w/K_u is unramified, so that $\mathrm{Gal}(M_w/K_u)$ is cyclic. Moreover, $\mathrm{Gal}(M_w/K_u)$ is isomorphic to some subgroup of $\mathrm{Gal}(M/K)$, which has exponent p, so that $\mathrm{Gal}(M_w/K_u)$ has exponent divisor of p and is therefore either trivial or cyclic of order p.

Let S' be the set of primes of L dividing some prime of S. Then, S' is a finite set of primes of L containing those that ramify in M, so that, since $\mathrm{Gal}(M/L)$ is Abelian, by Corollary 5.3.7, the Fröbenius elements $(\mathfrak{p}_v, M/L)$ with $v \notin S'$ generate $\mathrm{Gal}(M/L)$. Since

$$\mathrm{Gal}(M/L) \simeq (\mathbb{Z}/p\mathbb{Z})^t \ ,$$

the Galois group $\mathrm{Gal}(M/L)$ can be regarded as a t-dimensional vector space over $\mathbb{F}_p$, and we can choose primes $v_1, \ldots, v_t$ of L out of S' such that the Fröbenius elements $(\mathfrak{p}_{v_i}, M/L)$ form a basis of $\mathrm{Gal}(M/L)$. For each i, let w_i be a prime of M lying over v_i. We have the isomorphisms

$$\begin{aligned} \mathrm{Gal}(M_{w_i}/L_{v_i}) &\to G_{w_i}(M/L) \\ \sigma &\mapsto \sigma|_M \ , \end{aligned}$$

where the decomposition groups $G_{w_i}(M/L)$ are generated by the Fröbenius elements $(\mathfrak{p}_{v_i}, M/L)$. Since these elements have order p, as they form a basis of $\mathrm{Gal}(M/L)$, we deduce that M_{w_i}/L_{v_i} is cyclic of order p. Therefore, taking into account the discussion at the beginning of the proof, if, for each i, we define u_i as the prime of K lying under v_i, then $L_{v_i} = K_{u_i}$, so that

$$G_{w_i}(M/L) = G_{w_i}(M/K)$$

and

$$(\mathfrak{p}_{u_i}, M/K) = (\mathfrak{p}_{v_i}, M/L) \, .$$

Hence, the set $T = \{u_1, \ldots, u_t\}$ satisfies the property of the lemma. □

Lemma 5.4.7. With the previous definitions and assumptions, an element $a \in U(S)$ becomes a p-th power in L if and only if it becomes a p-th power in K_u for all $u \in T$ (T is any set of primes of K satisfying the property of the previous lemma).

Proof. Since T is disjoint from S, the primes in T are unramified in M. Then, since the corresponding Fröbenius elements form a basis of $\mathrm{Gal}(M/L)$, we know that, for any $u \in T$, $L_v = K_u$ for any prime $v|u$ of L and M_w/K_u is cyclic of order p for any prime $w|u$ of M.

Hence, it is clear that, if $a \in U(S)$ becomes a p-th power in L, so also does in K_u for every $u \in T$.

Conversely, assume that $a \in U(S)$ becomes a p-th power in K_u for each $u \in T$. Then, $(\mathfrak{p}_u, M/K)$ fixes $a^{1/p} \in M$ for all $u \in T$ (because $(\mathfrak{p}_u, M/K)$ is the restriction to M of the Fröbenius element of the extension M_w/K_u, where w is any prime of M dividing u). Since these Fröbenius elements generate $\mathrm{Gal}(M/L)$, we deduce that $a^{1/p}$ belongs to L and so a is a p-th power in L. □

Lemma 5.4.8. With the previous definitions and assumptions, the subgroup

$$E = \prod_{u \in S} K_u^{\times p} \times \prod_{u \in T} K_u^{\times} \times \prod_{u \notin S \cup T} U_u$$

of $\mathbb{I}_K$ is contained in $\mathrm{Nm}_{L/K}\mathbb{I}_L$.

Proof. Take any $\alpha = (\alpha_u)_u \in E$. We will find some $\beta = (\beta_v)_v \in \mathbb{I}_L$ such that $\mathrm{Nm}_{L/K}\beta = \alpha$. For any prime u of K and any prime $v|u$ of L, the local Artin map gives an isomorphism

$$K_u^{\times}/\mathrm{Nm}_{L_v/K_u} L_v^{\times} \to \mathrm{Gal}(L_v/K_u)\,.$$

Since $\mathrm{Gal}(L_v/K_u)$ is isomorphic to a subgroup of $\mathrm{Gal}(L/K)$, it has exponent a divisor of p, so that $K_u^{\times p} \subseteq \mathrm{Nm}_{L_v/K_u} L_v^{\times}$. Then, for each prime $u \in S$, we choose some prime $v_u|u$ of L and we define β_{v_u} such that $\mathrm{Nm}_{L_{v_u}/K_u}\beta_{v_u} = \alpha_u$ and $\beta_v = 1$ for all other $v|u$. Now, for the primes $u \in T$, we have $L_v = K_u$ for all $v|u$, so we need only take $\beta_v = \alpha_u$ for one of the primes $v|u$ and $\beta_v = 1$ for the other primes dividing u. Finally, since all primes out of S are unramified in L, for any $u \notin S$ and any prime $v|u$ of L, the norm map

$$\mathrm{Nm}_{L_v/K_u} : U_v \to U_u$$

is exhaustive, so, for each $u \notin S \cup T$, we need only take β_v to be a preimage of α_u under this map for one of the primes $v|u$ and $\beta_v = 1$ for the other primes dividing u. □

We want to prove the second inequality for the extension L/K, i.e. we want to prove that $[\mathbb{I}_K : K^{\times} \cdot \mathrm{Nm}_{L/K}\mathbb{I}_L]$ divides $[L : K] = p^r$. By the previous lemma, $K^{\times}E$ is a subgroup of $K^{\times} \cdot \mathrm{Nm}_{L/K}\mathbb{I}_L$, so that

$$[\mathbb{I}_K : K^{\times}E] = [\mathbb{I}_K : K^{\times} \cdot \mathrm{Nm}_{L/K}\mathbb{I}_L][K^{\times} \cdot \mathrm{Nm}_{L/K}\mathbb{I}_L : K^{\times}E]\,,$$

and, consequently, it suffices to prove that $[\mathbb{I}_K : K^{\times}E]$ divides p^r. This will be now our aim.

Lemma 5.4.9. With the previous definitions and assumptions, the map

$$U(S) \to \prod_{u \in T} U_u/U_u^p\,,$$

(defined in the natural way) is surjective.

Proof. By Lemma 5.4.7, the kernel of this map is $H = U(S) \cap L^{\times p}$. Observe that,

$$U(S)/H = U(S)/U(S) \cap L^{\times p} \simeq U(S) \cdot L^{\times p}/L^{\times p}\,.$$

Since $M = L(U(S)^{1/p})$ is the Abelian extension of L with exponent a divisor of p corresponding to the subgroup $U(S) \cdot L^{\times p}/L^{\times p}$ of $L^\times/L^{\times p}$ (see Proposition A.0.4),

$$[M : L] = [U(S) \cdot L^{\times p} : L^{\times p}] ,$$

so that we get

$$|U(S)/H| = [M : L] = p^t .$$

On the other hand, by the proof of Lemma 2.3.9,

$$|U_u/U_u^p| = \frac{p}{|p|_u} .$$

Since T is disjoint with S, which contains all infinite primes and all primes dividing p, $|p|_u = 1$ for all $u \in T$, so that we get

$$\left| \prod_{u \in T} U_u/U_u^p \right| = \prod_{u \in T} |U_u/U_u^p| = p^t .$$

Hence,

$$|U(S)/H| = \left| \prod_{u \in T} U_u/U_u^p \right| ,$$

which implies that the given map is surjective. □

Lemma 5.4.10. With the previous definitions and assumptions,

$$K^\times \cap E = U(S \cup T)^p .$$

Proof. The inclusion $U(S \cap T)^p \subseteq K^\times \cap E$ is clear, so we will focus on proving the inclusion $K^\times \cap E \subseteq U(S \cap T)^p$.

Let $a \in K^\times \cap E$. In order to prove that $a \in U(S \cup T)^p$, it suffices to show that it is a p-th power in $K^\times$ (since $a \in E$, it is a unit for any prime out of $S \cup T$ and so will be any p-th root of a, provided that it exists). To do that, we will consider the extension $L = K(a^{1/p})$ and use Lemma 5.3.4 to prove that $L = K$. More concretely, we will show that the subgroup

$$D = \prod_{u \in S} K_u^\times \times \prod_{u \in T} U_u^p \times \prod_{u \notin S \cap T} U_u$$

of $\mathbb{I}_K$ satisfies that $D \subseteq \mathrm{Nm}_{L/K}\mathbb{I}_L$ and $K^\times D = \mathbb{I}_K$ (so that, *a fortiori*, $K^\times D$ is dense in $\mathbb{I}_K$).

We begin by proving $D \subseteq \mathrm{Nm}_{L/K}\mathbb{I}_L$. Take $\alpha = (\alpha_u)_u \in D$.

For $u \in S$, since $a \in E$, a is a p-th power in K_u, so that $L_v = K_u(a^{1/p}) = K_u$ for all prime $v|u$ of L.

For every prime u of K, and any prime $v|u$ of L, the local Artin map gives an isomorphism

$$K_u^\times/\mathrm{Nm}_{L_v/K_u} L_v^\times \to \mathrm{Gal}(L_v/K_u) .$$

Since $\mathrm{Gal}(L_v/K_u)$ is isomorphic to a subgroup of $\mathrm{Gal}(L/K)$ (the decomposition group of v), it must divide p, so that, by the previous isomorphism, $[K_u^\times : \mathrm{Nm}_{L_v/K_u} L_v^\times]$ is also a divisor of p. This implies that any p-th power in $K_u^\times$ is the norm of some element of $L_v^\times$. Therefore, since

$\alpha \in D$, for $u \in T$, the component $\alpha_u \in K_u$ is the norm an element of L_v, where v is any prime of L dividing u.

For $u \notin S \cup T$, a is a unit in K_u, because $a \in E$, and so also is p, because S contains all primes dividing p. Therefore, pa is a unit in K_u, so that, by Proposition A.0.5, we know that $L_v = K_u(a^{1/p})$ is unramified over K_u, where v is any prime of L dividing u. Therefore, the norm map

$$\mathrm{Nm}_{L_v/K_u} : U_v \to U_u$$

is surjective, so that α_u is the norm of some element of $L_v^\times$.

From these considerations it easily follows that $\alpha \in \mathrm{Nm}_{L/K}\mathbb{I}_L$, so that we can conclude $D \subseteq \mathrm{Nm}_{L/K}\mathbb{I}_L$.

Now, observe that

$$\mathbb{I}_K^S/D = \prod_{u\in T} U_u/U_u^p\,.$$

Therefore,

$$\mathbb{I}_K^S = \bigsqcup_{\chi\in\Lambda} \chi D$$

for a set Λ of representatives of $\prod_{u\in T} U_u/U_u^p$, which by the previous lemma can be taken from $U(S)$ and so

$$\mathbb{I}_K^S = U(S)\cdot D\,.$$

Then, since S contains a set of generators Cl_K,

$$\mathbb{I}_K = K^\times \cdot \mathbb{I}_K^S = K^\times \cdot U(S)\cdot D = K^\times D\,,$$

where for the last equality we have used the previous proposition. □

Lemma 5.4.11. Let A, B and C be subgroups of the same Abelian group, and assume that $B \subseteq A$. Then

$$[AC : BC][A\cap C : B\cap C] = [A : B]\,.$$

Proof. Consider the diagram

$$\begin{array}{ccccccc} & & B\cap C & \longrightarrow & B & \longrightarrow & BC/C \longrightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & A\cap C & \longrightarrow & A & \longrightarrow & AC/C \end{array}$$

with the obvious maps. It is clearly commutative and the rows are clearly exact, so we may apply the snake lemma. Since the vertical arrows are injective and the last arrow in the second row is surjective, we obtain the exact sequence

$$0 \longrightarrow A\cap C/B\cap C \longrightarrow A/B \longrightarrow AC/BC \longrightarrow 0\,.$$

Thus,

$$|A/B| = |A\cap C/B\cap C|\cdot|AC/BC|\,,$$

which implies the statement. □

The following proposition completes the proof of the second inequality.

Proposition 5.4.12. With the previous definitions and assumptions,

$$\left[\mathbb{I}_K : K^\times E\right] = p^r \,.$$

Proof. Since S contains a set of generators of Cl_K, we have $\mathbb{I}_K = K^\times \cdot \mathbb{I}_K^{S\cup T}$. Therefore, applying the previous lemma, we get

$$\left[\mathbb{I}_K : K^\times E\right] = \left[K^\times \mathbb{I}_K^{S\cup T} : K^\times E\right] = \frac{\left[\mathbb{I}_K^{S\cup T} : E\right]}{\left[K^\times \cap \mathbb{I}_K^{S\cup T} : K^\times \cap E\right]} \,.$$

By definition,

$$\mathbb{I}_K^{S\cup T} = \prod_{u\in S} K_u^\times \times \prod_{u\in T} K_u^\times \times \prod_{u\notin S\cup T} U_u^\times$$

and

$$E = \prod_{u\in S} K_u^{\times p} \times \prod_{u\in T} K_u^\times \times \prod_{u\notin S\cup T} U_u^\times \,.$$

Therefore,

$$\mathbb{I}_K^{S\cup T}/E \simeq \prod_{u\in S} K_u^\times/K_u^{\times p} \,.$$

Hence, we get

$$\left[\mathbb{I}_K^{S\cup T} : E\right] = \prod_{u\in S} \left[K_u^\times : K_u^{\times p}\right] \,,$$

which, if we recall that K contains a primitive p-th root of unity and apply Lemma 2.3.9, becomes

$$[\mathbb{I}_K^{S\cup T} : E] = \prod_{u\in S} \frac{p^2}{|p|_u} = \frac{p^{2s}}{\prod_{u\in S}|p|_u} \,.$$

Since S contains all infinite primes and all primes dividing p, we have $|p|_u = 1$ for all $u \notin S$, so that

$$\prod_{u\in S} |p|_u = \prod_u |p|_u = 1 \,,$$

where the second sum runs through all primes of K and so the last equality is simply the product formula. In this way, we obtain

$$\left[\mathbb{I}_K^{S\cup T} : E\right] = p^{2s} \,.$$

Now, clearly $K^\times \cap \mathbb{I}_K^{S\cup T} = U(S\cup T)$, and, from Lemma 5.4.10, we know $K^\times \cap E = U(S\cup T)^p$, so that

$$\left[K^\times \cap \mathbb{I}_K^{S\cup T} : K^\times \cap E\right] = \left[U(S\cup T) : U(S\cup T)^p\right] \,.$$

In the same way as we did for $U(S)$ in the discussion previous to Lemma 5.4.6, we obtain

$$U(S\cup T)/U(S\cup T)^p \simeq (\mathbb{Z}/p\mathbb{Z})^{s+t} \,,$$

so that

$$\left[K^\times \cap \mathbb{I}_K^{S\cup T} : K^\times \cap E\right] = p^{s+t} \,.$$

Finally, putting all together, we get

$$\left[\mathbb{I}_K : K^\times E\right] = \left[K^\times \mathbb{I}_K^{S\cup T} : K^\times E\right] = \frac{\left[\mathbb{I}_K^{S\cup T} : E\right]}{\left[K^\times \mathbb{I}_K^{S\cup T} \cap : K^\times E\right]} = \frac{p^{2s}}{p^{s+t}} = p^r \,.$$

□

5.5 The Reciprocity Law

References: [Mil13]

We have already proved the Second Inequality, which states that for any number field K and for any finite Galois extension L of K of degree n,

$$\left[\mathbb{I}_K : K^\times \mathbb{I}_L\right] \leqslant n\,.$$

Therefore, if we prove that, for any finite Abelian extension L/K, the map

$$\phi_{L/K} : \mathbb{I}_K \to \mathrm{Gal}(L/K)$$

is surjective and $K^\times \cdot \mathrm{Nm}_{L/K}\mathbb{I}_L \subseteq \ker \phi_{L/K}$, it follows that the induced surjective map

$$\phi_{L/K} : \mathbb{I}_K/(K^\times \cdot \mathrm{Nm}_{L/K}\mathbb{I}_L) \to \mathrm{Gal}(L/K)$$

is actually an isomorphism and hence

$$\ker \phi_{L/K} = K^\times \cdot \mathrm{Nm}_{L/K}\mathbb{I}_L\,.$$

In fact, we already know that $\phi_{L/K}$ is surjective because of Corollary 5.3.7 (for finite unramified primes v, the local Artin map sends any local uniformizing parameter in K_v to the corresponding Fröbenius element). Note also that we have already proved that $\mathrm{Nm}_{L/K}\mathbb{I}_L \subseteq \ker \phi_{L/K}$ throughout the proof of Proposition 5.1.1. Therefore, to complete the proof of the Reciprocity Law, we need only prove that, for any finite Abelian extension L/K,

$$\phi_{L/K}(K^\times) = 1\,.$$

We begin by proving this result for cyclotomic extensions of $\mathbb{Q}$. To this end, we need a explicit description of the local Artin maps corresponding to cyclotomic extensions of $\mathbb{Q}_p$, where p denotes any prime. Let ζ_n denote a primitive n-th root of unity, and consider the extension $\mathbb{Q}_p(\zeta_n)$. We know that the Galois group $\mathrm{Gal}(\mathbb{Q}_p(\zeta_n)/\mathbb{Q}_p)$ (and in general that of any cyclotomic extension) can be regarded as a subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$ by considering the injective homomorphism

$$\begin{aligned}\mathrm{Gal}(\mathbb{Q}_p(\zeta_n)/\mathbb{Q}_p) &\to (\mathbb{Z}/n\mathbb{Z})^\times\\ \sigma &\mapsto [i(\sigma)]\,,\end{aligned}$$

where $\sigma(\zeta) = \zeta^{i(\sigma)}$. Since, if $n = l_1^{r_1}\dots l_t^{r_t}$ is the factorization of n in prime factors,

$$\mathbb{Q}_p(\zeta_n) = \mathbb{Q}_p(\zeta_{l_1^{r_1}})\dots\mathbb{Q}_p(\zeta_{l_t^{r_t}})$$

and

$$\phi_{\mathbb{Q}_p(\zeta_n)/\mathbb{Q}_p}(a)|_{\mathbb{Q}_p(\zeta_{l_i^{r_i}})} = \phi_{\mathbb{Q}_p(\zeta_{l_i^{r_i}})/\mathbb{Q}_p}(a)$$

for any $a \in \mathbb{Q}_p^\times$ and for any $i = 1,\dots,t$, we may restrict to the case $n = l^r$ for some prime l, and we can obviously assume $n \geqslant 3$.

If $p = \infty$, then $\mathbb{Q}_p = \mathbb{R}$, $\mathbb{Q}_p(\zeta_{l^r}) = \mathbb{C}$ and the isomorphism

$$\phi_{\mathbb{C}/\mathbb{R}} : \mathbb{R}^\times/\mathrm{Nm}_{\mathbb{C}/\mathbb{R}}\mathbb{C}^\times \to \mathrm{Gal}(\mathbb{C}/\mathbb{R})$$

shows that positive numbers are mapped to the identity whereas negative numbers are mapped to complex conjugation, i.e.

$$\begin{aligned}\phi_{\mathbb{C}/\mathbb{R}} : \mathbb{R}^\times &\to \mathrm{Gal}(\mathbb{C}/\mathbb{R}) \subseteq (\mathbb{Z}/l^r\mathbb{Z})^\times \\ a &\mapsto [\mathrm{sign}(a)]\,.\end{aligned}$$

If p is a finite prime different from l, then the extension $\mathbb{Q}_p(\zeta_{l^r})/\mathbb{Q}_p$ is unramified, so that

$$\phi_{\mathbb{Q}_p(\zeta_{l^r})/\mathbb{Q}_p} : \mathbb{Q}_p^\times \to \mathrm{Gal}(\mathbb{Q}_p(\zeta_{l^r})/\mathbb{Q}_p)$$

is the map sending units to the identity and the local uniformizing parametre p to the Fröbenius element $(p, \mathbb{Q}_p(\zeta_{l^r})/\mathbb{Q}_p)$, i.e.

$$\begin{aligned}\phi_{\mathbb{Q}_p(\zeta_{l^r})/\mathbb{Q}_p} : \mathbb{Q}_p^\times &\to \mathrm{Gal}(\mathbb{Q}_p(\zeta_{l^r})/\mathbb{Q}_p) \\ a = up^s &\mapsto [p^s]\end{aligned}$$

where u denotes a unit in $\mathbb{Q}_p$. Finally, if $p = l$, the extension $\mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^r})/\mathbb{Q}_p)$ is totally ramified and we have

$$\begin{aligned}\phi_{\mathbb{Q}_p(\zeta_{p^r})/\mathbb{Q}_p} : \mathbb{Q}_p^\times &\to \mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^r})/\mathbb{Q}_p) \\ a = up^s &\mapsto [u^{-1}]\end{aligned}$$

where in the right we are taking the residue modulo p of the p-adic number u (this description of the local Artin map for this particular case can be found in [Mil13, p. 43]).

Now, let us use this description of the local Artin maps to show that $\phi_{\mathbb{Q}(\zeta_{l^r})/\mathbb{Q}}(\mathbb{Q}^\times) = 1$ (which implies the desired result for all cyclotomic extensions of $\mathbb{Q}$). Since $\mathbb{Q}^\times$ is generated by -1 and the prime numbers, we need only check that $\phi_{\mathbb{Q}(\zeta_{l^r})/\mathbb{Q}}(a) = 1$ when a is either -1 or a prime number. We know that for cyclotomic extensions of $\mathbb{Q}$, the map

$$\begin{aligned}\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) &\to (\mathbb{Z}/n\mathbb{Z})^\times \\ \sigma &\mapsto [i(\sigma)]\end{aligned}$$

is in fact an isomorphism, and it is obvious that an element in $\mathrm{Gal}(\mathbb{Q}_p(\zeta_n)/\mathbb{Q}_p)$ associated to $[m] \in (\mathbb{Z}/n\mathbb{Z})^\times$ restricts to the element in $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ associated to the same element $[m] \in (\mathbb{Z}/n\mathbb{Z})^\times$. Therefore:

1. If $a = -1$, the above description shows that $\phi_{\infty,\mathbb{Q}(\zeta_{l^r})/\mathbb{Q}}(-1) = [-1]$, $\phi_{l,\mathbb{Q}(\zeta_{l^r})/\mathbb{Q}}(-1) = [-1]$ and $\phi_{p,\mathbb{Q}(\zeta_{l^r})/\mathbb{Q}}(-1) = [1]$ for any finite prime $p \neq l$, so that

$$\phi_{\mathbb{Q}(\zeta_{l^r})/\mathbb{Q}}(-1) = \prod_p \phi_{p,\mathbb{Q}(\zeta_{l^r})/\mathbb{Q}}(-1) = [1]\,.$$

2. If $a = l$, then $\phi_{p,\mathbb{Q}(\zeta_{l^r})/\mathbb{Q}}(l) = [1]$ for all prime p, so that

$$\phi_{\mathbb{Q}(\zeta_{l^r})/\mathbb{Q}}(l) = \prod_p \phi_{p,\mathbb{Q}(\zeta_{l^r})/\mathbb{Q}}(l) = [1]\,.$$

3. If $a = q$, where q is a prime number different from l, then we have $\phi_{\infty,\mathbb{Q}(\zeta_{l^r})/\mathbb{Q}}(q) = [1]$, $\phi_{l,\mathbb{Q}(\zeta_{l^r})/\mathbb{Q}}(q) = [q^{-1}]$, $\phi_{q,\mathbb{Q}(\zeta_{l^r})/\mathbb{Q}}(q) = [q]$ and $\phi_{p,\mathbb{Q}(\zeta_{l^r})/\mathbb{Q}}(q) = [1]$ for any finite prime $p \neq q, l$, so that, again,

$$\phi_{\mathbb{Q}(\zeta_{l^r})/\mathbb{Q}}(q) = \prod_p \phi_{p,\mathbb{Q}(\zeta_{l^r})/\mathbb{Q}}(q) = [1]\,.$$

Lemma 5.5.1. Let K be a number field, let M be a finite extension of K and let L be a finite extension of M. Then, if $\phi_{L/K}(K^\times) = 1$, it also holds $\phi_{M/K}(K^\times) = 1$.

Proof. The result follows from the property

$$\phi_{M/K}(\alpha) = \phi_{L/K}(\alpha)|_M \quad \text{for all } \alpha \in \mathbb{I}_K \, .$$

□

Lemma 5.5.2. Let K be a number field and let L and M be finite Abelian extensions of K. Then, if $\phi_{L/K}(K^\times) = 1$, it also holds that $\phi_{LM/M}(M^\times) = 1$.

Proof. Let $N = LM$. Let v be a prime of M, let $w|v$ be a prime of N and let t and u be the primes of K and L, respectively, lying under w. Consider the diagram

$$\begin{array}{ccccc} M_v^\times & \xrightarrow{\phi_{N_w/M_v}} & \mathrm{Gal}(N_w/M_v) & \xrightarrow{\sigma \mapsto \sigma|_N} & \mathrm{Gal}(N/M) \\ \downarrow{\scriptstyle \mathrm{Nm}_{M_v/K_t}} & & \downarrow{\scriptstyle \sigma \mapsto \sigma|_{L_u}} & & \downarrow{\scriptstyle \sigma \mapsto \sigma|_L} \\ K_t^\times & \xrightarrow{\phi_{L_u/K_t}} & \mathrm{Gal}(L_u/K_t) & \xrightarrow{\sigma \mapsto \sigma|_L} & \mathrm{Gal}(L/K) \end{array} \, .$$

The left square can be obtained from the commutative diagram

$$\begin{array}{ccc} M_v^\times & \xrightarrow{\phi_{N_w/M_v}} & \mathrm{Gal}(N_w/M_v) \\ \downarrow{\scriptstyle \mathrm{Nm}_{M_v/K_t}} & & \downarrow \\ K_t^\times & \xrightarrow{\phi_{N_w/K_t}} & \mathrm{Gal}(N_w/K_t) \end{array}$$

by composing the right vertical arrow and the bottom horizontal arrow with the restriction map

$$\begin{aligned} \mathrm{Gal}(N_w/K_t) &\to \mathrm{Gal}(L_u/K_t) \\ \sigma &\mapsto \sigma|_{L_u} \, , \end{aligned}$$

so that it is itself commutative. The right square is also clearly commutative, so that the whole diagram is commutative and we obtain the commutative diagram

$$\begin{array}{ccc} M_v^\times & \xrightarrow{\phi_{v,N/M}} & \mathrm{Gal}(N/M) \\ \downarrow{\scriptstyle \mathrm{Nm}_{M_v/K_t}} & & \downarrow{\scriptstyle \sigma \mapsto \sigma|_L} \\ K_t^\times & \xrightarrow{\phi_{t,L/K}} & \mathrm{Gal}(L/K) \end{array} \, .$$

From these commutative diagrams we obtain the commutative diagram

$$\begin{array}{ccc} \mathbb{I}_M & \xrightarrow{\phi_{N/M}} & \mathrm{Gal}(N/M) \\ \downarrow{\scriptstyle \mathrm{Nm}_{M/K}} & & \downarrow{\scriptstyle \sigma \mapsto \sigma|_L} \\ \mathbb{I}_K & \xrightarrow{\phi_{L/K}} & \mathrm{Gal}(L/K) \end{array} \, .$$

Since $\mathrm{Nm}_{M/K}M^\times \subseteq K^\times$, under the assumption $\phi_{L/K}(K^\times) = 1$ we have

$$\phi_{N/M}(M^\times)|_L = \phi_{L/K}(\mathrm{Nm}_{M/K}(M^\times)) = 1$$

and, since the restriction map

$$\begin{aligned} \mathrm{Gal}(LM/M) &\to \mathrm{Gal}(L/K) \\ \sigma &\mapsto \sigma_L \end{aligned}$$

is injective, we get

$$\phi_{N/M}(M^\times) = 1\,.$$

□

Note that, as a consequence of the previous lemmas, and taking into account the previous discussion about the cyclotomic extensions of $\mathbb{Q}$, we have that $\phi_{L/K}(K^\times) = 1$ for every subextension L of a cyclotomic extension of a number field K.

Lemma 5.5.3. Let K be a number field, and let S be a finite set of finite primes of K. Then, for every integer $m > 0$, there exists a cyclic subextension L of a cyclotomic extension of K such that m divides $[L^v : K_v]$ for all prime $v \in S$.

Proof. We begin by proving the lemma in the case $K = \mathbb{Q}$. In this case, for any prime l,

$$\mathrm{Gal}(\mathbb{Q}(\zeta_{l^r})/\mathbb{Q}) \simeq (\mathbb{Z}/l^r\mathbb{Z})^\times \simeq \begin{cases} C_{l-1} \times C_{l^{r-1}} & \text{if } l \neq 2 \\ C_2 \times C_{2^{r-2}} & \text{if } l = 2 \end{cases}.$$

In both cases, let $H = \langle([1],[0])\rangle$, and let $L(l^r) = \mathbb{Q}(\zeta_{l^r})^H$. Then,

$$\mathrm{Gal}(L(l^r)/\mathbb{Q}) \simeq \begin{cases} C_{l^{r-1}} & \text{if } l \neq 2 \\ C_{2^{r-2}} & \text{if } l = 2 \end{cases}.$$

The prime l totally ramifies in $\mathbb{Q}(\zeta_{l^r})$ (i.e. the corresponding ramification index and inertia degree are $e_l = \phi(l^r)$ and $f_l = 1$). Therefore, we have $[\mathbb{Q}_l(\zeta_{l^r}) : \mathbb{Q}_l] = e_l f_l = \phi(l^r)$. Any prime $p \neq l$ is totally unramified in $\mathbb{Q}(\zeta_{l^r})$, so that the ramification index is $e_p = 1$ and the inertia degree is the order of the Fröbenius element defined by $\zeta_{l^r} \mapsto \zeta_{l^r}^p$, which is the minimum positive integer t such that $l^r | p^t - 1$. Therefore, we have $[\mathbb{Q}_p(\zeta_{l^r}) : \mathbb{Q}_p] = e_p f_p = t$. In both cases, the degree of the extension $\mathbb{Q}_p(\zeta_{l^r})/\mathbb{Q}_p$ becomes arbitrarily large as r grows. Consider the completion $L(l^r)^p = L(l^r)\mathbb{Q}_p$. Since $[\mathbb{Q}_p(\zeta_{l^r}) : L(l^r)^p] \leqslant [\mathbb{Q}(\zeta_{l^r}) : L(l^r)] = |H|$, we deduce that the degree of the extension $L(l^r)^p/\mathbb{Q}_p$ also becomes arbitrarily large as r grows. Moreover, we know that the Galois group $\mathrm{Gal}(L(l^r)^p/\mathbb{Q}_p)$ is isomorphic to a subgroup of $\mathrm{Gal}(L(l^r)/\mathbb{Q})$, so that it must be cyclic of order a power of l.

Now, given an integer $m > 0$, and a finite set S of finite primes of $\mathbb{Q}$, take, for each prime l dividing m, the extension $L(l^{r_l})$, with r_l sufficiently large so that, for each prime $p \in S$, the largest l-power dividing m also divides $[L(l^{r_l})^p : \mathbb{Q}_p]$. Consider the extension $M = \prod_{l|m} L(l^{r_l})$. Since the extensions $L(l^{r_l})$ for $l|m$ have cyclic Galois group of order a power of a different prime,

$$\mathrm{Gal}(M/\mathbb{Q}) \simeq \prod_{l|m} \mathrm{Gal}(L(l^{r_l})/\mathbb{Q})$$

is also cyclic and, for each prime p,

$$\mathrm{Gal}(M^p/\mathbb{Q}_p) \simeq \prod_{l|m} \mathrm{Gal}(L(l^{r_l})^p/\mathbb{Q}_p)\,,$$

so that clearly $m|[M^p : \mathbb{Q}_p]$ for each $p \in S$.

Now, let K be any number field, let S be a finite set of finite primes of K and let m be an integer. Let $m' = m[K : \mathbb{Q}]$, and let S' be the set of primes of $\mathbb{Q}$ lying under some prime of S. Then, there exists a cyclic subextension L' of a cyclotomic extension of $\mathbb{Q}$ such that m' divides $[L'^p : \mathbb{Q}_p]$ for all prime $p \in S'$. Take $L = KL'$. It is a subextension of a cyclotomic extension of K, and it is cyclic because its Galois group is isomorphic to a subgroup of $\mathrm{Gal}(L'/\mathbb{Q})$. Let v be a prime in S, and let p be coresponding prime of $\mathbb{Q}$. Since m' divides $[L'^v : \mathbb{Q}_p]$, we have

$$m[K : \mathbb{Q}] \mid [L^v : \mathbb{Q}_p] = [L^v : K_v][K_v : \mathbb{Q}_p]\,,$$

which, since $[K_v : \mathbb{Q}_p] \mid [K : \mathbb{Q}]$, shows that m divides $[L^v : K_v]$.

□

Let us introduce some notations. For a Galois extension L/K, we will write $H^r(L/K)$ for $H^r(\mathrm{Gal}(L/K), L^\times)$, and, for any field K, we will write $H^r(/K)$ for $H^r(\mathrm{Gal}(K^{\mathrm{s}}/K), K^{\mathrm{s}\times})$.

Lemma 5.5.4. Let K be a number field and L a Galois extension of K. Then, there is an injective homomorphism

$$H^2(L/K) \hookrightarrow \bigoplus_v H^2(L^v/K_v)\,.$$

Proof. First assume that L/K is finite, and let $G = \mathrm{Gal}(L/K)$. Consider the short exact sequence

$$1 \longrightarrow L^\times \longrightarrow \mathbb{I}_L \longrightarrow C_L \longrightarrow 1\,.$$

By Theorem 5.4.1, $H^1(G, C_L) = 0$, so that from the induced long exact cohomology sequence we get that the sequence

$$0 \longrightarrow H^2(L/K) \longrightarrow H^2(G, \mathbb{I}_L)$$

is exact, so that the homomorphism

$$H^2(L/K) \to H^2(G, \mathbb{I}_L)$$

is injective. Composing this homomorphism with the isomorphism

$$H^2(L/K) \simeq \bigoplus_v H^2(L^v/K_v)$$

given by Proposition 4.3.6, we obtain the injective homomorphism

$$\begin{aligned} H^2(L/K) &\to \bigoplus_v H^2(L^v/K_v) \\ \varphi &\mapsto (\varphi_v)_v \end{aligned}$$

where $\varphi \mapsto \varphi_v$ is the homomorphism induced by the pair of compatible homomorphisms

$$\begin{aligned} \mathrm{Gal}(L^v/K_v) &\to \mathrm{Gal}(L/K) \\ \sigma &\mapsto \sigma|_L \end{aligned}$$

and

$$L^\times \hookrightarrow L^{v\times}$$

(this description can be proved by following the proof of Proposition 4.3.6).

Now, suppose that L is an infinite Galois extension. In this case, we have

$$H^2(L/K) \simeq \varinjlim H^2(G/H, L^{H\times}),$$

where the direct limit is taken over the open subgroups H of G of finite index. This is equivalent to taking the direct limit over the finite Galois subextensions F of L. Using this fact, and applying the result for the finite case,

$$H^2(L/K) \simeq \varinjlim H^2(\mathrm{Gal}(F/K), F^\times) \hookrightarrow \varinjlim \bigoplus_v H^2(F^v/K_v) \simeq$$
$$\simeq \bigoplus_v \varinjlim H^2(F^v/K_v) \simeq \bigoplus_v H^2(L^v/K_v)$$

(remember that when L/K is finite, then L_w is not the completion of L with respect to the valuation w, but the direct union of the completions of the finite subextensions), and it is straightforward, following the previous chain of isomorphisms, that, as in the finite case, the injective homomorphism

$$H^2(L/K) \to \bigoplus_v H^2(L^v/K_v)$$
$$\varphi \mapsto (\varphi_v)_v$$

arises at each component through the pair of compatible homomorphisms

$$\mathrm{Gal}(L^v/K_v) \to \mathrm{Gal}(L/K)$$
$$\sigma \mapsto \sigma|_L$$

and

$$L^\times \hookrightarrow L^v .$$

□

Lemma 5.5.5. Let K be a number field. Then, for any $\varphi \in H^2(/K)$, there exists a cyclic subextension L of a cyclotomic extension of K such that φ maps to zero in $H^2(/L)$ under the restriction map.

Proof. For any finite Galois extension L/K, using the description of the maps involved, it is easy to see that the diagram

$$\begin{array}{ccc} H^2(/K) & \xrightarrow{\quad\mathrm{Res}\quad} & H^2(/L) \\ \downarrow & & \downarrow \\ \bigoplus_v H^2(K^{\mathrm{al},v}/K_v) & \xrightarrow{\bigoplus_v \mathrm{Res}_v} & \bigoplus_v H^2(K^{\mathrm{al},v}/L^v) \end{array}$$

commutes. Let $(\varphi_v)_v$ be the image of φ in $\bigoplus_v H^2(K^{\mathrm{al},v}/K_v)$. Since the diagram commutes and the vertical arrows are injective, in order that φ map to zero in $H^2(/L)$ it is sufficient that $(\varphi_v)_v$ map to zero in $\bigoplus_v H^2(K^{\mathrm{al},v}/L^v)$, i.e. it is sufficient that $\mathrm{Res}_v\varphi_v = 0$ for all primes v of K. Observe that $\varphi_v \neq 0$ only for a finite number of primes v. Let S be the set of finite primes such that $\varphi_v \neq 0$, let $\mathrm{inv}_{K_v}(\varphi_v) \in \frac{1}{n_v}\mathbb{Z}/\mathbb{Z}$ and let m be the lcm of the n_v for $v \in S$. By Lemma 5.5.3,

there exists a cyclic subextension L of a cyclotomic extension of K such that n divides $[L^v : K_v]$ for all $v \in S$. Therefore,

$$\mathrm{inv}_{L^v}(\mathrm{Res}_v \varphi_v) = [L^v : K_v] \, \mathrm{inv}_{K_v}(\varphi_v) = 0 \, ,$$

which, because of the injectivity of the invariant map, implies that $\mathrm{Res}_v \varphi_v = 0$. The extension L is obtained by adjoining extensions of the form $L(l^r)$ for some prime l (we are following the notations used in the proof of Lemma 5.5.3). For $l = 2$, and for $r \geqslant 3$, we can always take $H = \langle [2^{r-1} + 1] \rangle \subseteq (\mathbb{Z}/2^r\mathbb{Z})^\times$, so that $L(2^r)$ is a complex number field, and, therefore, we have that φ_v becomes zero in $H^2(K^{\mathrm{al},v}/L^v)$ also for infinite primes v. □

Given a number field K, and a prime v of K, we will use the notation inv_v for the composite of the homomorphism

$$H^2(/K) \to H^2(K^{\mathrm{al},v}/K_v)$$

obtained from the pair of compatible homomorphisms

$$\mathrm{Gal}(K^{\mathrm{al},v}/K_v) \simeq G_v(K^{\mathrm{al}}/K) \hookrightarrow \mathrm{Gal}(K^{\mathrm{al}}/K)$$

and

$$K^{\mathrm{al}} \hookrightarrow K^{\mathrm{al},v} \, ,$$

and the homomorphism $\mathrm{inv}_{K^{\mathrm{al}} K_v / K_v}$. Forcing a little bit the notation, for a finite extension L/K, we will also denote by inv_v the composite

$$H^2(L/K) \xrightarrow{\mathrm{Inf}} H^2(/K) \xrightarrow{\mathrm{inv}_v} \mathbb{Q}/\mathbb{Z} \, .$$

Lemma 5.5.6. Let L/K be a finite Abelian extension of number fields.

1. If $\sum_v \mathrm{inv}_v(\alpha) = 0$ for all $\alpha \in H^2(L/K)$, then $\phi_{L/K}(K^\times) = 1$.
2. If L/K is cyclic and $\phi_{L/K}(K^\times) = 1$, then $\sum_v \mathrm{inv}_v(\alpha) = 0$ for all $\alpha \in H^2(L/K)$.

Proof. Let $G = \mathrm{Gal}(L/K)$. Any character $\chi \in \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z})$ can be regarded as an element in $H^1(G, \mathbb{Q}/\mathbb{Z})$. Let $\delta : H^1(G, \mathbb{Q}/\mathbb{Z}) \to H^2(G, \mathbb{Z})$ be the connecting map from the exact sequence

$$0 \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Q} \longrightarrow \mathbb{Q}/\mathbb{Z} \longrightarrow 0 \, .$$

Consider the diagram

$$\begin{array}{ccccc} K^\times & \longrightarrow & \mathbb{I}_K & \xrightarrow{\phi_{L/K}} & G \\ \downarrow{\scriptstyle \cup \delta\chi} & & \downarrow{\scriptstyle \cup \delta\chi} & & \downarrow{\scriptstyle \chi} \\ H^2(G, L^\times) & \longrightarrow & H^2(G, \mathbb{I}_L) & \longrightarrow & \mathbb{Q}/\mathbb{Z} \end{array} \, ,$$

where the second arrow in the second row is given by the composite

$$H^2(G, \mathbb{I}_L) \xrightarrow{\simeq} \bigoplus_v H^2(G^v, L^{v\times}) \xrightarrow{\sum_v \mathrm{inv}_{L^v/K_v}} \mathbb{Q}/\mathbb{Z} \, .$$

The first vertical arrow, which is cup product with $\delta\chi$, is given by

$$\begin{aligned} K^\times &\to H^2(G, L^\times) \\ x &\mapsto \left[(\sigma,\tau) \mapsto x \otimes_{\mathbb{Z}} \delta\chi(\sigma,\tau) = x^{\delta\chi(\sigma,\tau)}\right], \end{aligned}$$

and, in the same way, the second vertical arrow is given by

$$\begin{aligned} \mathbb{I}_K &\to H^2(G, \mathbb{I}_L) \\ x &\mapsto \left[(\sigma,\tau) \mapsto x \otimes_{\mathbb{Z}} \delta\chi(\sigma,\tau) = x^{\delta\chi(\sigma,\tau)}\right]. \end{aligned}$$

Using this description, it is obvious that the first square in the diagram commutes. For the second square, take any $(\alpha_v)_v \in \mathbb{I}_K$. Going down in the diagram, we obtain $\varphi \in H^2(G, \mathbb{I}_L)$ given by $\varphi(\sigma,\tau) = (\alpha_w^{\delta(\sigma,\tau)})_w$, where $\alpha_w = \alpha_v$ if $w|v$. Under the isomorphism

$$H^2(G, \mathbb{I}_L) \to \bigoplus_v H^2(G^v, L^{v\times}),$$

the element φ is mapped to $(\varphi_v)_v$, with $\varphi_v(\sigma,\tau) = \alpha_v^{\delta\chi_v(\sigma,\tau)}$ for all $\sigma,\tau \in \mathrm{Gal}(L^v/K_v)$, i.e. $\varphi_v = \alpha_v \cup \delta\chi_v$, where χ_v is the restriction of χ to $\mathrm{Gal}(L^v/K_v) \simeq G_v(L/K)$. Hence, going first down and then right, we obtain

$$\sum_v \mathrm{inv}_{L^v/K_v}(\alpha_v \cup \delta\chi).$$

Going first right and then down we obtain

$$\sum_v \chi_v(\phi_{L^v/K_v}(\alpha_v)),$$

and both expressions are equal because of Proposition 3.3.5.

Observe that the composite of the bottom arrows is given by $\alpha \mapsto \sum_v \mathrm{inv}_v(\alpha)$. Since the whole diagram is commutative, then if $\sum_v \mathrm{inv}_v(\alpha) = 0$ for all $\alpha \in H^2(L/K)$, we deduce that $\chi(\phi_{L/K}(K^\times)) = 0$ for all $\chi \in \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z})$, so that $\phi_{L/K}(K^\times) = 1$. Conversely, assuming that L/K is cyclic, we can obviously choose an injective character $\chi \in \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z})$. Then, cup product with $\delta\chi$ is an isomorphism (see the remark following Proposition 1.9.8), so that, if $\phi_{L/K}(K^\times) = 1$, we deduce that $\sum_v \mathrm{inv}_v(\alpha) = 0$ for all $\alpha \in H^2(L/K)$. □

Because of the first part of the previous lemma, if we prove that, for all finite Abelian extensions of number fields L/K, it holds that $\sum_v \mathrm{inv}_v(\alpha) = 0$ for all $\alpha \in H^2(L/K)$, we will have proved the Reciprocity Law. Note also that the second part of the lemma, together with the previous results, implies that this condition holds for all cyclic subextensions of cyclotomic extensions of number fields. We will use this fact to prove that it holds for all finite Galois extensions of number fields. Since the local invariant maps inv_v are defined as the composite of the corresponding inflation map and the map inv_v defined for the algebraic closure of K, this is achieved through the following lemma.

Lemma 5.5.7. Let K be a number field. Then,

$$\sum_v \mathrm{inv}_v(\alpha) = 0 \quad \text{for all } \alpha \in H^2(/K).$$

Proof. Because of the previous discussion, if $\alpha \in H^2(/K)$ comes by inflation from an element of $H^2(L/K)$ for some cyclic subextension of a cyclotomic extension of K, then $\sum_v \mathrm{inv}_v(\alpha) = 0$. Therefore, we need only prove that every $\alpha \in H^2(/K)$ comes by inflation from such an element.

Take any $\alpha \in H^2(/K)$. By Lemma 5.5.5, there exists a cyclic subextension L of a cyclotomic extension of K such that α maps to zero in $H^2(/L)$ under the restriction map. Since, by Hilbert's theorem 90, $H^1(/L) = 0$, we get the inflation-restriction exact sequence

$$0 \longrightarrow H^2(L/K) \xrightarrow{\text{Inf}} H^2(/K) \xrightarrow{\text{Res}} H^2(/L) \,,$$

which shows that α comes by inflation of some element in $H^2(L/K)$. □

We conclude this section by using the Reciprocity Law to prove the following proposition.

Proposition 5.5.8. Let K be a number field, let L_1 and L_2 be finite Abelian extensions of K within the same maximal Abelian extension K^{ab}, and let $N_1 = \mathrm{Nm}_{L_1/K} C_{L_1}$ and $N_2 = \mathrm{Nm}_{L_2/K} C_{L_2}$. Then:

1. $L_1 \subseteq L_2 \Leftrightarrow N_1 \supseteq N_2$.
2. $\mathrm{Nm}_{L_1 \cap L_2/K} C_{L_1 \cap L_2} = N_1 N_2$.
3. $\mathrm{Nm}_{L_1 L_2/K} C_{L_1 L_2} = N_1 \cap N_2$.

Proof. The Reciprocity Law implies that, for any finite Abelian extension L/K, we have that $\mathrm{Nm}_{L/K} C_L = \ker \phi_K(\cdot)|_L$. From this observation, it follows

$$L_1 \subseteq L_2 \Rightarrow N_1 = \ker \phi_K(\cdot)|_{L_1} \supseteq \ker \phi_K(\cdot)|_{L_2} = N_2$$

and

$$\mathrm{Nm}_{L_1 L_2/K} C_{L_1 L_2} = \ker \phi_K(\cdot)|_{L_1 L_2} = \ker \phi_K(\cdot)_{L_1} \cap \ker \phi_K(\cdot)|_{L_2} = N_1 \cap N_2$$

(which is statement 3). The isomorphism

$$\phi_{L_1 L_2/K} : C_K / \mathrm{Nm}_{L_1 L_2/K} C_{L_1 L_2} \to \mathrm{Gal}(L_1 L_2/K)$$

restricts to isomorphisms

$$\phi_{L_1 L_2/K} : \mathrm{Nm}_{L_1/K} C_{L_1} / \mathrm{Nm}_{L_1 L_2/K} C_{L_1 L_2/K} \to \mathrm{Gal}(L_1 L_2/L_1)$$

and

$$\phi_{L_1 L_2/K} : \mathrm{Nm}_{L_2/K} C_{L_2} / \mathrm{Nm}_{L_1 L_2/K} C_{L_1 L_2/K} \to \mathrm{Gal}(L_1 L_2/L_2)\,,$$

so that,

$$N_1 \supseteq N_2 \Leftrightarrow \mathrm{Gal}(L_1 L_2/L_1) \supseteq \mathrm{Gal}(L_1 L_2/L_2)\,,$$

which, by Galois theory, implies statement 1.

We also know, from Galois theory, that

$$\mathrm{Gal}(L_1 L_2/L_1) \cdot \mathrm{Gal}(L_1 L_2/L_2) = \mathrm{Gal}(L_1 L_2/L_1 \cap L_2)\,,$$

so that we get the isomorphism

$$\phi_{L_1 L_2/K} : \mathrm{Nm}_{L_1/K} C_{L_1} \cdot \mathrm{Nm}_{L_2/K} C_{L_2} / \mathrm{Nm}_{L_1 L_2/K} C_{L_1 L_2/K} \to \mathrm{Gal}(L_1 L_2/L_1 \cap L_2)\,,$$

which, by the Reciprocity Law, implies statement 2. □

5.6 The Existence Theorem

References: [Mil13], [Tat67]

Throughout this section K will be a number field. We have seen that, given a finite Abelian extension L/K, the global Artin map induces an isomorphism

$$\phi_{L/K} : C_K/\mathrm{Nm}_{L/K}C_L \to \mathrm{Gal}(L/K)\,.$$

Since the map

$$\phi_{L/K} : C_K \to \mathrm{Gal}(L/K)$$

is surjective, this is equivalent to saying that $\mathrm{Nm}_{L/K}C_L = \phi^{-1}(\mathrm{Gal}(K^{\mathrm{ab}}/L))$. Therefore, the subgroups of C_K of the form $N = \mathrm{Nm}_{L/K}C_L$ for some finite Abelian extension L/K are precisely the preimages by ϕ of the open subgroups of $\mathrm{Gal}(K^{\mathrm{ab}}/K)$. We will refer to this kind of subgroups as *normic* subgroups. We will say that $N = \mathrm{Nm}_{L/K}C_L$ is the *normic subgroup for* L and that L is the *class field* of $N = \mathrm{Nm}_{L/K}C_L$. It is clear that normic subgroups are of finite index, and they are also open because of Proposition 4.2.4. What we want to prove in this section is that, in fact, every open subgroup of C_K of finite index is a normic subgroup, so that we get a bijection between finite Abelian extensions of K and open subgroups of C_K of finite index.

Lemma 5.6.1. Let L be a finite Galois extension of K and let M and M' be finite Abelian extensions of L such that there exists a K-isomorphism $\sigma : M \to M'$. Then, for every $x \in C_L$, we have

$$\phi_{M'/L}(\sigma x) = \sigma \circ \phi_{M/L}(x) \circ \sigma^{-1}\,.$$

Proof. Let L' be the image of L in M' under σ. Let L^{ab} and $L^{\mathrm{ab}'}$ be maximal Abelian extensions containing M and M', respectively. Let $\tilde{\sigma}$ be an extension of σ to an isomorphism $\tilde{\sigma} : L^{\mathrm{ab}} \to L^{\mathrm{ab}'}$. Then, we must have

$$\phi'_{L'}(\sigma x) = \tilde{\sigma} \circ \phi_L \circ \tilde{\sigma}^{-1}$$

for all $x \in C_L$, so that

$$\phi'_{M'/L'}(\sigma x) = \sigma \circ \phi_{M/L} \circ \sigma^{-1}$$

for all $x \in C_L$. Since L/K is Galois, we have $L' = L$ in M', so that we get the desired result. □

Lemma 5.6.2. Let L be a Galois extension of K with Galois group $G = \mathrm{Gal}(L/K)$ and let M be an Abelian extension of L. If $\mathrm{Nm}_{M/L}C_M$ is invariant under the action of G, then M is a Galois extension of K.

Proof. Let K^{al} be an algebraic closure of K containing M. We shall prove that, given any K-embedding

$$\sigma : M \to K^{\mathrm{al}}\,,$$

we have $\sigma M = M$, which implies that M/K is Galois.

So let $\sigma : M \to K^{\mathrm{al}}$ be a K-embedding and let $M' = \sigma M$. First note that M' is an Abelian extension of L. In fact, $\sigma L = L$ because L is a Galois extension of K, and therefore

$$\mathrm{Aut}(M'/L) = \mathrm{Aut}(M'/\sigma L) = \sigma\mathrm{Aut}(M/L)\sigma^{-1} = \sigma\mathrm{Gal}(M/L)\sigma^{-1}\,.$$

Thus, by the previous lemma, we get a commutative diagram

$$\begin{array}{ccc} C_L & \xrightarrow{\sigma|_L} & C_L \\ \downarrow{\scriptstyle \phi(\cdot)|_M} & & \downarrow{\scriptstyle \phi(\cdot)|_{M'}} \\ \mathrm{Gal}(M/L) & \xrightarrow{\tau \mapsto \sigma\tau\sigma^{-1}} & \mathrm{Gal}(M'/L) \end{array} .$$

From this diagram, it is clear that, if $\mathrm{Nm}_{M/L}C_M = \ker \phi(\cdot)|_M$ is invariant under G, then

$$\ker \phi(\cdot)|_M = \ker \phi(\cdot)|_{M'} = \ker \phi(\cdot)|_{MM'} .$$

But then the Reciprocity Law implies $M = MM' = M'$. □

Lemma 5.6.3. Let N and P be subgroups of C_K, with $N \subseteq P$. Then, if N is normic, so is P.

Proof. Let $N = \mathrm{Nm}_{L/K}C_L$. By the Reciprocity Law, we have an isomorphism

$$\phi_{L/K} = \phi(\cdot)|_L : C_K/N \to \mathrm{Gal}(L/K) .$$

Let M be the fixed field of $\phi_{L/K}(P/N)$. Then, by Galois theory, we have $\phi_{L/K}(P/N) = \mathrm{Gal}(L/M)$, so that from the previous isomorphism we get a new isomorphism

$$\phi_{M/K} = \phi(\cdot)|_M : C_K/P \simeq \frac{C_K/N}{P/N} \to \mathrm{Gal}(L/K)/\mathrm{Gal}(L/M) \simeq \mathrm{Gal}(M/K) ,$$

which, by the Reciprocity Law, implies $P = \mathrm{Nm}_{M/K}C_M$. □

Lemma 5.6.4. Assume that K contains a primitive p-th root of unity for some prime number p. Then, any open subgroup N of C_K such that the quotient group is finite with exponent p is a norm group.

Proof. Let N be an open subgroup of C_K such that C_K/N is finite of exponent p. Let N' be the preimage of N in $\mathbb{I}_K$. It is also open, and, since $\mathbb{I}_K/N' \simeq C_K/N$, we see that $\mathbb{I}_K/N'$ also has exponent p. Because N' is open, there is a finite set S of primes of K containing the infinite primes such that

$$\prod_{v\in S}\{1\} \times \prod_{v\notin S} U_v \subseteq N' ,$$

and, because $\mathbb{I}_K/N'$ has exponent p, we also have $\mathbb{I}_K^p \subseteq N'$. Therefore, the subgroup

$$E = \prod_{v\in S} K_v^{\times p} \times \prod_{v\notin S} U_v$$

is contained in N', so that

$$K^\times E/K^\times \subseteq N .$$

We can obviously assume that the set S contains all primes dividing p. By Lemma 5.6.3, to prove that N is normic it suffices to prove that $K^\times E/K^\times$ is normic.

Let $L = K(U(S)^{1/p})$. As we did in the discussion previous to Lemma 5.4.6, we can prove that $[L : K] = p^s$, where $s = |S|$. Also, as we did in Lemma 5.4.8, we can prove that $E \subseteq \mathrm{Nm}_{L/K}\mathbb{I}_L$, and, as in Proposition 5.4.12, we can prove that $[\mathbb{I}_K : K^\times E] = p^s$. Since, by the Reciprocity Law, we have $\left[\mathbb{I}_K : K^\times \mathrm{Nm}_{L/K}\mathbb{I}_L\right] = [L : K] = p^s$, we deduce that $K^\times E = K^\times \mathrm{Nm}_{L/K}\mathbb{I}_L$, and, consequently, that $K^\times E/K^\times = \mathrm{Nm}_{L/K}C_L$. □

Lemma 5.6.5. Let L/K be a cyclic extension and let N be a subgroup of C_K. Then, if $\mathrm{Nm}_{L/K}^{-1}(N)$ is normic in C_L, so is N in C_K.

Proof. Let $N' = \mathrm{Nm}_{L/K}^{-1}(N)$, and let M be the class field of N', i.e. $N' = \mathrm{Nm}_{M/L}C_M$. Let $C = \mathrm{Gal}(L/K)$, and let $H = \mathrm{Gal}(M/L)$, which are both Abelian groups. Since, for all $\sigma \in C$, and for all $x \in C_L$, we have $\mathrm{Nm}_{L/K}(\sigma x) = \mathrm{Nm}_{L/K}(x)$, we see that N' is invariant under C and, consequently, by Lemma 5.6.2, we deduce that M is Galois over K. Let $G = \mathrm{Gal}(M/K)$. We claim that G is Abelian. Since H is Abelian and $G/H \simeq C$ is cyclic, it suffices to see that H is contained in the centre of G. Using the isomorphism

$$\phi_{M/L} : C_L/\mathrm{Nm}_{M/L}C_M \to H\,,$$

we need to show that, for all $x \in C_L$ and for all $\sigma \in G$,

$$\phi_{M/L}(x) = \sigma\phi_{M/L}(x)\sigma^{-1}\,.$$

Now, applying Lemma 5.6.1, we need to see that

$$\phi_{M/L}(x) = \phi_{M/L}(\sigma x)$$

for all $\sigma \in C$ and for all $x \in C_L$. But this follows easily because $\mathrm{Nm}_{L/K}(\sigma x/x) = 1$, so that $\sigma x/x \in N'$ and, consequently, $\phi_{M/L}(\sigma x/x) = 1$.

Therefore, we see that M/K is an Abelian extension, so that $\mathrm{Nm}_{M/K}C_M$ is normic. This subgroup is contained in N by transitivity of the norms, and hence N is normic by Lemma 5.6.3. □

Theorem 5.6.6. Then, every open subgroup of C_K of finite index is normic.

Proof. Consider any open subgroup N of C_K of finite index. We will argue by induction on the index $n = [C_K : N]$. If $n = 1$, then the statement is trivial (we have $N = C_K = \mathrm{Nm}_{K/K}C_K$). For $n > 1$, let p be any prime dividing n. Let K' be an extension of K resulting from adjoining a p-th root of unity. Such an extension is cyclic, so that, by the previous lemma, we need only prove that $N' = \mathrm{Nm}_{K'/K}^{-1}N$ is normic in $C_{K'}$. This subgroup is open because the norm map is continuous. The map

$$\mathrm{Nm}_{K'/K} : C_{K'} \to C_K/N$$

has clearly kernel N', so that $[C_{K'} : N']$ divides n. If $[C_{K'} : N'] \neq n$, then we are already done by the induction hypothesis, so let us assume that $[C_{K'} : N'] = n$. Let $N_1' \supseteq N'$ be a subgroup of $C_{K'}$ of index $[C_{K'} : N_1'] = p$. Since N' is open and $N' \subseteq N_1'$, we see that N_1' is also open. By Lemma 5.6.4, the subgroup N_1' is normic in $C_{K'}$. Let L be its class field, and let $P = \mathrm{Nm}_{L/K'}^{-1}(N')$. Since L/K' is cyclic of order p, again by the previous lemma, to prove that N' is normic in $C_{K'}$ it suffices to prove that P is normic in C_L. This subgroup is open because the norm map is continuous. The map

$$\mathrm{Nm}_{L/K'} : C_L \to C_K'/N'$$

has clearly kernel P and image N_1'/N', so that $[C_L : P] = n/p$ and P is normic by the induction hypothesis. □

Remark 28. The uniqueness part of the Existence Theorem is an obvious consequence of Proposition 5.5.8.

Chapter 6

Ideal-theoretic global class field theory

6.1 Moduli

References: [Mil13], [Neu99]

Definition 6.1.1. A *modulus* in K is a formal product $\mathfrak{m} = \prod_{\mathfrak{p}} \mathfrak{p}^{m(\mathfrak{p})}$ over all primes $\mathfrak{p}$ of K, with exponents $m(\mathfrak{p}) \geqslant 0$ which are all zero except for finitely many primes $\mathfrak{p}$, and, for infinite primes $\mathfrak{p}$, they are zero if $\mathfrak{p}$ is complex and they may be zero or one if $\mathfrak{p}$ is real.

We will usually write $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$, where $\mathfrak{m}_0$ stands for the finite primes and $\mathfrak{m}_\infty$ for the infinite primes.

Given a modulus $\mathfrak{m}$, for every $\mathfrak{p}|\mathfrak{m}$ we define $W_{\mathfrak{m}}(\mathfrak{p})$ as $\mathbb{R}^+$, if $\mathfrak{p}$ is an infinite real prime, and $1 + \hat{\mathfrak{p}}^{m(\mathfrak{p})}$ if $\mathfrak{p}$ is a finite prime. Note that, in both cases, the set $W_{\mathfrak{m}}(\mathfrak{p})$ is an open neighborhood of 1 in $K_{\mathfrak{p}}$. When $\mathfrak{p} \nmid \mathfrak{m}$, then we define $W_{\mathfrak{m}}(\mathfrak{p}) = U_{\mathfrak{p}}$.

We will denote by $\mathbb{I}_K(\mathfrak{m})$ the subgroup of $\mathbb{I}_K$ comprised of the idèles α such that, for every prime $\mathfrak{p}|\mathfrak{m}$, $\alpha_{\mathfrak{p}} \in W_{\mathfrak{m}}(\mathfrak{p})$. The set of the idèles which satisfy that, in addition, $\alpha_{\mathfrak{p}} \in \mathcal{O}_{\mathfrak{p}}^{\times}$ for all finite primes will be denoted by $W_{\mathfrak{m}}$. Define also $P_{K,1}(\mathfrak{m}) = K^{\times} \cap \mathbb{I}_K(\mathfrak{m})$. The set of principal ideals in I_K generated by elements of $P_{K,1}(\mathfrak{m})$ will be also denoted by $P_{K,1}(\mathfrak{m})$. It is not difficult to see that this is in fact the same as the subgroup of I_K generated by the principal ideals of the form $\alpha\mathcal{O}_K$ for some $\alpha \in \mathcal{O}_K$ such that $\alpha \equiv 1 \pmod{\mathfrak{m}_0}$ and $\sigma(\alpha) > 0$ for all real prime σ dividing $\mathfrak{m}_\infty$ (here σ refers both to the real prime and the associated real K-embedding). Let $I_K(\mathfrak{m})$ be the set of ideals in I_K generated by the set of finite primes not dividing $\mathfrak{m}$. Clearly, $P_{K,1}(\mathfrak{m}) \subseteq I_K(\mathfrak{m})$. Define $Cl_K(\mathfrak{m}) = I_K(\mathfrak{m})/P_{K,1}(\mathfrak{m})$.

Lemma 6.1.2. The inclusion map

$$\mathbb{I}_K(\mathfrak{m}) \to \mathbb{I}_K$$

induces an isomorphism

$$\mathbb{I}_K(\mathfrak{m})/P_{K,1}(\mathfrak{m}) \to \mathbb{I}_K/K^{\times}\,.$$

Proof. Clearly, the kernel of the map

$$\mathbb{I}_K(\mathfrak{m}) \to \mathbb{I}_K/K^{\times}$$

is $K^\times \cap \mathbb{I}_K(\mathfrak{m}) = P_{K,1}(\mathfrak{m})$, so we need only prove surjectivity to obtain the desired isomorphism. To this end, we need only apply the weak approximation theorem. Take any element in $\mathbb{I}_K/K^\times$, and assume that it corresponds to the class of some idèle $\alpha \in \mathbb{I}_K$. By the weak approximation theorem, we can choose $a \in K^\times$ which is arbitrarily close to $\alpha_\mathfrak{p}$ for all prime $\mathfrak{p}|\mathfrak{m}$. Therefore, we can choose $a \in K^\times$ such that $\alpha_\mathfrak{p}/a$ is arbitrarily close to 1 for all $\mathfrak{p}|\mathfrak{m}$, and, in particular, we can achieve that $\alpha_\mathfrak{p}/a$ lies in $W_\mathfrak{m}(\mathfrak{p})$ for all $\mathfrak{p}|\mathfrak{m}$. Hence, $a^{-1}\alpha \in \mathbb{I}_K(\mathfrak{m})$. Since this element lies in the same class of $\mathbb{I}_K/K^\times$ as α, we see that the map is surjective. □

We can easily see that the canonical surjective homomorphism

$$\mathrm{id} : \mathbb{I}_K \to I_K$$

restricts to a surjective homomorphism

$$\mathrm{id} : \mathbb{I}_K(\mathfrak{m}) \to I_K(\mathfrak{m}) .$$

Lemma 6.1.3. The surjective homomorphism

$$\mathrm{id} : \mathbb{I}_K(\mathfrak{m}) \to I_K(\mathfrak{m})$$

induces an isomorphism

$$\mathrm{id} : \mathbb{I}_K(\mathfrak{m})/(P_{K,1}(\mathfrak{m}) \cdot W_\mathfrak{m})) \to Cl_K(\mathfrak{m}) .$$

Proof. Consider the maps

$$P_{K,1}(\mathfrak{m}) \xrightarrow{\ i\ } \mathbb{I}_K(\mathfrak{m}) \xrightarrow{\ \mathrm{id}\ } I_K(\mathfrak{m})$$

where i denotes the inclusion map. It is clear that the kernel of id in the previous diagram is the set of $\alpha \in \mathbb{I}_K(\mathfrak{m})$ such that $\alpha_\mathfrak{p}$ is a unit in $K_\mathfrak{p}$ for all finite prime $\mathfrak{p}$ not dividing $\mathfrak{m}$, i.e. $\ker \mathrm{id} = W_\mathfrak{m}$. Also note that id is clearly surjective, so that $\mathrm{coker id} = \{1\}$. Therefore, the last part of the exact sequence provided by the kernel-cokernel lemma is

$$W_\mathfrak{m} \longrightarrow \mathbb{I}_K(\mathfrak{m})/P_{K,1}(\mathfrak{m}) \longrightarrow Cl_K(\mathfrak{m}) \longrightarrow 1 ,$$

whereby the desired result follows. □

Definition 6.1.4. Given a modulus $\mathfrak{m}$, the *congruence subgroup for* $\mathfrak{m}$ is the group

$$C_K(\mathfrak{m}) = W_\mathfrak{m} \cdot K^\times/K^\times .$$

The *ray class group for* $\mathfrak{m}$ is the quotient group

$$C_K/C_K(\mathfrak{m}) .$$

Proposition 6.1.5. There exists an isomorphism

$$C_K/C_K(\mathfrak{m}) \to Cl_K(\mathfrak{m}) .$$

Proof. First of all, observe that

$$C_K/C_K(\mathfrak{m}) = \frac{\mathbb{I}_K/K^\times}{W_m \cdot K^\times/K^\times} \simeq \mathbb{I}_K/(W_\mathfrak{m} \cdot K^\times)\,.$$

Now, using Lemma 6.1.2 and Lemma 6.1.3,

$$\mathbb{I}_K/(W_\mathfrak{m} \cdot K^\times) \simeq \mathbb{I}_K(\mathfrak{m})/(W_\mathfrak{m} \cdot P_{K,1}(\mathfrak{m})) \simeq Cl_K(\mathfrak{m})\,.$$

□

Remark 29. The groups $C_K/C_K(\mathfrak{m})$ and $Cl_K(\mathfrak{m})$ are both often referred to as the *ray class group for* $\mathfrak{m}$.

Proposition 6.1.6. The open subgroups of C_K are precisely those containing some $C_K(\mathfrak{m})$ as a subgroup, and they all have finite index.

Proof. The subgroup $C_K(\mathfrak{m})$ is open since its preimage in $\mathbb{I}_K$ contains the open subgroup $W_\mathfrak{m}$ and so is itself open. It also has finite index in C_K. In fact, we have

$$[C_K : C_K(\mathfrak{m})] = \left[C_K : \mathbb{I}_K^{S_\infty} \cdot K^\times/K^\times\right]\left[\mathbb{I}_K^{S_\infty} \cdot K^\times/K^\times : W_\mathfrak{m} \cdot K^\times/K^\times\right]\,,$$

so that, if h denotes the class number,

$$[C_K : C_K(\mathfrak{m})] \leqslant h\left[\mathbb{I}_K^{S_\infty} : W_\mathfrak{m}\right] = h\prod_{\mathfrak{p}|\mathfrak{m}}[U_\mathfrak{p} : W_\mathfrak{m}(\mathfrak{p})]\,,$$

which is clearly finite. Obviously, since every congruence group $C_K(\mathfrak{m})$ is open and of finite index in C_K, so is any subgroup containing some $C_K(\mathfrak{m})$.

Conversely, let N be an open subgroup of C_K, and let N' be its preimage in $\mathbb{I}_K$. Then, the group N' must contain some open neighborhood of 1, i.e. it must contain some subset of the form

$$\prod_{\mathfrak{p}\in S} W_\mathfrak{p} \times \prod_{\mathfrak{p}\notin S} U_\mathfrak{p}\,,$$

where S is a finite set of primes of K and the sets $W_\mathfrak{p}$ are open neighborhoods of 1 in $K_\mathfrak{p}^\times$. For complex infinite primes, the elements in $W_\mathfrak{p}$ generate $K_p^\times$; for real infinite primes, the elements in $W_\mathfrak{p}$ generate at least $\mathbb{R}^+$, and, for finite primes in S, there is some $n_\mathfrak{p}$ such that $1+\mathfrak{p}^{n_\mathfrak{p}} \subseteq W_\mathfrak{p}$. Therefore, we see that N' contains some $W_\mathfrak{m}$ (with $S(\mathfrak{m}) \subseteq S$), and, consequently, the subgroup N contains some congruence subgroup $C_K(\mathfrak{m})$. □

For a set of primes S of K, we will denote by $I_K(S)$ the subgroup of I_K generated by the finite prime ideals not in S and by $\mathbb{I}_K(S)$ the subgroup of $\mathbb{I}_K$ comprised of those idèles $\alpha \in \mathbb{I}_K$ such that $\alpha_v = 1$ for all $v \in S$.

Definition 6.1.7. Let S be a finite set of primes of K, and let G be a finite Abelian group. Then, we say that a homomorphism

$$\psi : I_K(S) \to G$$

admits a modulus if there exists a modulus $\mathfrak{m}$ such that the finite primes dividing $\mathfrak{m}$ are precisely the finite primes in S and $\psi(P_{K,1}(\mathfrak{m})) = 1$.

Proposition 6.1.8. Let S be a finite set of primes of K, and let G be a finite Abelian group (which we provide with the discrete topology). If a homomorphism

$$\psi : I_K(S) \to G$$

admits a modulus, then there exists a unique continuous homomorphism

$$\phi : \mathbb{I}_K \to G$$

such that

1. $\phi(K^\times) = 1$.
2. $\phi(\alpha) = \psi(\mathrm{id}(\alpha))$ for all $\alpha \in \mathbb{I}_K(S)$.

Conversely, for any continuous homomorphism

$$\phi : \mathbb{I}_K \to G$$

such that $\phi(K^\times) = 1$, there exists a finite set of primes S and a homomorphism

$$\psi : I_K(S) \to G$$

such that ϕ arises from ψ in this way.

Proof. Consider a homomorphism

$$\psi : I_K(S) \to G$$

and assume that it admits a modulus, so that there exists some modulus $\mathfrak{m}$ whose finite primes are precisely those in S such that $\psi(P_{K,1}(\mathfrak{m})) = 1$. Therefore, ψ induces a homomorphism

$$\psi : Cl_K(\mathfrak{m}) \to G\,.$$

Define ϕ as the composite

$$\mathbb{I}_K \longrightarrow \mathbb{I}_K/K^\times \longrightarrow \mathbb{I}_K(\mathfrak{m})/P_{K,1}(\mathfrak{m}) \longrightarrow \mathbb{I}_K(\mathfrak{m})/(P_{K,1}(\mathfrak{m}) \cdot W_{\mathfrak{m}}) \longrightarrow Cl_K(\mathfrak{m}) \xrightarrow{\psi} G$$

where the second arrow is the inverse of the isomorphism from Lemma 6.1.2 and the fourth arrow is the isomorphism from Lemma 6.1.3. Clearly $W_{\mathfrak{m}} \subseteq \ker\phi$, so that, since $W_{\mathfrak{m}}$ is an open subgroup of $\mathbb{I}_K$, the map ϕ is continuous. It is also obvious from the definition that $\phi(K^\times) = 1$, and it is easy to see that any $\alpha \in \mathbb{I}_K(\mathfrak{m})$ is mapped to $\mathrm{id}(\alpha)$ in $Cl_K(\mathfrak{m})$ under the previous chain of maps, so that $\phi(\alpha) = \psi(\mathrm{id}(\alpha))$ for all $\alpha \in \mathbb{I}_K(\mathfrak{m})$ and, *a fortiori*, for any $\alpha \in \mathbb{I}_K(S)$.

To prove that this is the only continuous map satisfying the requirements in the statement, observe that these requirements determine ϕ on $\mathbb{I}_K(S) \cdot K^\times$, so that it suffices to see that this set is dense in $\mathbb{I}_K(S)$. But this is a consequence of the weak approximation theorem, as, for any $\alpha \in \mathbb{I}_K$, we can choose $a \in K^\times$ to be arbitrarily close to α_v for $v \in S$, so that, defining an idèle α' with $\alpha'_v = 1$ for $v \in S$ and $\alpha'_v = a^{-1}\alpha_v$ for all $v \notin S$, we can find an element $a\alpha' \in \mathbb{I}_K(S) \cdot K^\times$ arbitrarily close to α_v.

Now, suppose that we are given a continuous homomorphism

$$\phi : \mathbb{I}_K \to G$$

such that $\phi(K^\times) = 1$. Since it is continuous and we are considering the discrete topology in G, the kernel must be an open subgroup of $\mathbb{I}_K$. In particular, it must contain an open neighborhood of 1

$$\prod_{v\in S} V_v \times \prod_{v\notin S} U_v^\times$$

where S is a finite set of primes and the sets V_v are open neighborhoods of 1 in $K_v^\times$. Observe that, for finite primes $v \in S$, the set V_v must contain $1+\hat{\mathfrak{p}}_v^{n_v}$ for some $n_v \geqslant 0$, whereas for infinite primes v, the group $K_v^\times$ is isomorphic to either $\mathbb{R}^\times$ or $\mathbb{C}^\times$ and the connected component of 1, i.e. $\mathbb{R}^+$ or $\mathbb{C}^\times$, must be mapped to 1. Taking, for example, a modulus $\mathfrak{m}$ such that $\mathfrak{m}(\mathfrak{p}_\mathfrak{v}) = n_v$ for all finite primes $v \in S$ and $\mathfrak{m}(v) = 1$ for those real infinite primes for which only the connected component of 1 in $K_v^\times$ is mapped to 1, we see that $\phi(W_\mathfrak{m}) = 1$. Hence, since we already know that $\phi(K^\times) = 1$, we see that ϕ induces a homomorphism

$$\phi : \mathbb{I}_K(\mathfrak{m})/(P_{K,1}(\mathfrak{m}) \cdot W_\mathfrak{m}) \to G\,.$$

Now, take $S = S(\mathfrak{m})$ (i.e. the set of primes dividing $\mathfrak{m}$) and define $\psi : I_K(S) \to G$ as the composite

$$I_K(S) \longrightarrow Cl_K(\mathfrak{m}) \longrightarrow \mathbb{I}_K(\mathfrak{m})/(P_{K,1}(\mathfrak{m}) \cdot W_\mathfrak{m}) \xrightarrow{\phi} G$$

where the second arrow is the inverse of the isomorphism from Lemma 6.1.3. It is obvious that ψ admits the modulus $\mathfrak{m}$ and that it gives rise to ϕ. □

6.2 Ideal-theoretic formulation

References: [Cox13], [Mil13], [Neu86]

In this section, we will give a version of the main theorems of class field theory in terms of ideals.

Throughout this section K will always be a number field.

Proposition 6.2.1. Let $\mathfrak{m}$ be a modulus in K. Then, the group $Cl_K(\mathfrak{m})$ is finite.

Proof. This is a consequence of Proposition 6.1.5 and Proposition 6.1.6. □

Definition 6.2.2. Let $\mathfrak{m}$ be a modulus in K. A *congruence subgroup for* $\mathfrak{m}$ is a subgroup $H \subseteq I_K(\mathfrak{m})$ such that $P_{K,1}(\mathfrak{m}) \subseteq H \subseteq I_K(\mathfrak{m})$. In this case, the quotient $I_K(\mathfrak{m})/H$ is called a *generalized ideal class group for* $\mathfrak{m}$.

Now, we define the Artin map in terms of ideals.

Definition 6.2.3. Let L be an Abelian extension of K and let S be the set of finite primes of K ramifying in L. Then, the *(ideal-theoretic) Artin map for* $K \subseteq L$ is the group homomorphism

$$\psi_{L/K} : I_K(S) \to \mathrm{Gal}(L/K)$$

defined over the prime ideals $\mathfrak{p}$ in $I_K(S)$ as the Artin symbol $(\mathfrak{p}, L/K)$ and extended by multiplicativity.

Remark 30. For a finite extension of number fields L/K, we say that a finite prime $\mathfrak{p}$ of K ramifies in L if there is some prime $\mathfrak{P}$ of L lying above $\mathfrak{p}$ with ramification index $e_{\mathfrak{P}|\mathfrak{p}} > 1$. We will say that an infinite prime of K ramifies in L if it is real and has some extension to L which is complex. Obviously, when dealing with Galois extensions, if some extension to L of an infinite prime of K is complex, so are all the extensions of the same prime.

Theorem 6.2.4. (Reciprocity Law) Let L be a finite Abelian extension of K and let S be the set of finite primes of K ramifying in L. Then, the Artin map $\psi_{L/K}$ is surjective and admits a modulus (i.e. there exists a modulus $\mathfrak{m}$ such that the finite primes dividing $\mathfrak{m}$ are precisely those in S and $\psi_{L/K}(P_{K,1}(\mathfrak{m})) = 1$).

Proof. The surjectivity of the Artin map follows from Corollary 5.3.7. Let us see that it admits a modulus.

We know that the map

$$\phi_{L/K} : \mathbb{I}_K \to \mathrm{Gal}(L/K)$$

given by the global Artin map is continuous. Therefore, its kernel must contain $W_{\mathfrak{m}}$ for some modulus $\mathfrak{m}$. Recall that the map $\phi_{L/K}$ is defined by

$$\phi_{L/K}(\alpha) = \prod_v \phi_{v,L/K}(\alpha_v)\,,$$

where v runs through the primes of K. For the finite primes v that do not ramify in L, we know that $\phi_{v,L/K}(U_v) = 1$. Also note that, for infinite primes, the maps $\phi_{v,L/K}$ are trivial unless v is real and extends to complex primes in L. Therefore, the modulus $\mathfrak{m}$ can be taken so that the primes dividing $\mathfrak{m}$ are the primes of K which ramify in L (both finite and infinite primes). Note that $\mathfrak{m}$ must in fact be divisible by all such primes, as the local Artin maps for infinite ramified primes are not trivial (negative numbers are mapped to complex conjugation), and the local Artin maps for finite ramified primes do not act trivially on the units. For this modulus, it is straightforward to see that the diagram

$$\begin{array}{ccc} \mathbb{I}_K(\mathfrak{m}) & & \\ \Big\downarrow{\scriptstyle \mathrm{id}} & \searrow^{\phi_{L/K}} & \\ I_K(S) & \xrightarrow{\psi_{L/K}} & \mathrm{Gal}(L/K) \end{array}\,.$$

is commutative. Therefore, since $\phi_{L/K}(P_{K,1}(\mathfrak{m})) = 1$, we also have $\psi_{L/K}(P_{K,1}(\mathfrak{m})) = 1$. □

Remark 31. We have defined the Artin map for L/K on the group $I_K(S)$, where S denotes the set of finite primes of K which ramify in L. We can obviously restrict the Artin map to subgroups of the form $I_K(S')$, where S' is a finite set of primes of K containing those in S. We will denote these restricted maps by $\psi_{L/K,S'}$. These maps are also surjective (again, by Corollary 5.3.7) and admit a modulus (if $\psi_{L/K}$ admits the modulus $\mathfrak{m}$, we need only multiply this modulus by the finite primes in S' which are not in S).

Definition 6.2.5. Let L be a finite Abelian extension of K and let S be the set of finite primes of K ramifying in L. A modulus $\mathfrak{m}$ of K divisible by all primes in S is a *modulus of definition for* L/K if $\psi_{L/K}(P_{K,1}(\mathfrak{m})) = 1$.

Remark 32. If $\mathfrak{m}$ is a modulus of definition for L/K, then $P_{K,1}(\mathfrak{m}) \subseteq \ker \psi_{L/K,S(\mathfrak{m})}$, which means that $H = \ker \psi_{L/K,S(\mathfrak{m})}$ is a congruence subgroup for $\mathfrak{m}$ and $\mathrm{Gal}(L/K) \simeq I_K(\mathfrak{m})/H$ is a generalized ideal class group for $\mathfrak{m}$.

Lemma 6.2.6. Let L be a finite Abelian extension of K. A modulus $\mathfrak{m}$ of K is a modulus of definition for L/K if and only if $C_K(\mathfrak{m}) \subseteq \mathrm{Nm}_{L/K} C_L$.

Proof. By the idelic Reciprocity Law, we know that $C_K(\mathfrak{m}) \subseteq \mathrm{Nm}_{L/K} C_L$ if and only if $W_{\mathfrak{m}}$ is contained in the kernel of $\phi_{L/K} : \mathbb{I}_K \to \mathrm{Gal}(L/K)$. If this is the case, the proof of Theorem 6.2.4 shows that all ramified primes divide $\mathfrak{m}$ and $\psi_{L/K}(P_{K,1}(\mathfrak{m})) = 1$.

Conversely, if $\mathfrak{m}$ is a modulus of definition for L/K, then the map $\psi_{L/K,S(\mathfrak{m})}$ admits the modulus $\mathfrak{m}$. Therefore, by Proposition 6.1.8, there exists a unique continuous homomorphism $\phi : \mathbb{I}_K \to \mathrm{Gal}(L/K)$ such that $\phi(K^\times) = 1$ and $\phi(\alpha) = \psi(\mathrm{id}(\alpha))$ for all $\alpha \in \mathbb{I}_K(S(\mathfrak{m}))$. Since the Artin map $\phi_{L/K}$ satisfies these properties, the map given by the proposition is precisely $\phi_{L/K}$, and the construction in the proof of the proposition implies that $W_{\mathfrak{m}}$ is contained in the kernel of $\phi_{L/K}$. □

Theorem 6.2.7. Let L be a finite Abelian extension of K. Then, there exists a modulus $\mathfrak{f}$ of K such that:

1. Any prime of K ramifies in L if and only if it divides $\mathfrak{f}$.
2. A modulus $\mathfrak{m}$ in K is a modulus of definition for L/K if and only if $\mathfrak{f} \mid \mathfrak{m}$.

Proof. Observe that

$$\prod_{\lambda \in \Lambda} W_{\mathfrak{m}_\lambda} = W_{\gcd\{m_\lambda\}_{\lambda \in \Lambda}},$$

where Λ is a set of indices. Therefore, by the previous lemma, the gcd of the defining moduli for L/K is also a defining modulus for L/K. Also by the previous lemma (or by simply observing that, if $\mathfrak{m}_1 \mid \mathfrak{m}_2$, then $P_{K,1}(\mathfrak{m}_1) \supseteq P_{K,1}(\mathfrak{m}_2)$) this modulus satisfies the second statement. It also satisfies the first one, since in the proof of Theorem 6.2.4 we showed that there exists a modulus of definition which is only divided by the ramified primes. □

Definition 6.2.8. Let L be an Abelian extension of K. Then, the *conductor* of the extension L/K is the modulus $\mathfrak{f}$ from the previous theorem (it is clearly unique by the second condition in the theorem).

Proposition 6.2.9. Let L_1 and L_2 be finite Abelian extensions of K within the same maximal Abelian extension K^{ab}. Let S be a finite set of primes of K containing the finite primes that ramify in either L_1 or L_2. Then:

1. $L_1 \subseteq L_2 \Leftrightarrow \ker \psi_{L_1/K,S} \supseteq \ker \psi_{L_2/K,S}$.
2. $\ker \psi_{L_1 \cap L_2/K,S} = \ker \psi_{L_1/K,S} \cdot \ker \psi_{L_2/K,S}$.
3. $\ker \psi_{L_1 L_2/K,S} = \ker \psi_{L_1/K,S} \cap \ker \psi_{L_2/K,S}$.

Proof. Observe that $\psi_{L_1/K,S}(\cdot) = \psi_{L_1 L_2/K,S}(\cdot)|_{L_1}$ and $\psi_{L_2/K,S}(\cdot) = \psi_{L_1 L_2/K,S}(\cdot)|_{L_2}$, whereby we deduce statement 3.

The isomorphism

$$\psi_{L_1 L_2/K,S} : I_K(S)/\ker \psi_{L_1 L_2/K,S} \to \mathrm{Gal}(L_1 L_2/K)$$

restricts to isomorphisms

$$\psi_{L_1 L_2/K,S} : \ker \psi_{L_1/K,S}/\ker \psi_{L_1 L_2/K,S} \to \mathrm{Gal}(L_1 L_2/L_1)$$

and

$$\psi_{L_1 L_2/K,S} : \ker \psi_{L_2/K,S}/\ker \psi_{L_1 L_2/K,S} \to \mathrm{Gal}(L_1 L_2/L_2),$$

so that

$$\ker \psi_{L_1/K,S} \supseteq \ker \psi_{L_2/K,S} \Leftrightarrow \mathrm{Gal}(L_1L_2/L_1) \supseteq \mathrm{Gal}(L_1L_2/L_2)\,,$$

which, by Galois theory, implies statement 1.

We also know, from Galois theory, that

$$\mathrm{Gal}(L_1L_2/L_1) \cdot \mathrm{Gal}(L_1L_2/L_2) = \mathrm{Gal}(L_1L_2/L_1 \cap L_2)\,,$$

so that we get the isomorphism

$$\phi_{L_1L_2/K,S} : \ker \phi_{L_1/K,S} \cdot \ker \phi_{L_2/K,S} / \ker \psi_{L_1L_2/K} \to \mathrm{Gal}(L_1L_2/L_1 \cap L_2)\,,$$

which implies statement 2. □

Proposition 6.2.10. Let L be a finite Abelian extension of K with Galois group $G = \mathrm{Gal}(L/K)$. If $\mathfrak{m}$ is a modulus of definition for L/K, then the Artin map $\psi_{L/K,S(\mathfrak{m})}$ induces an isomorphism

$$\psi_{L/K,S(\mathfrak{m})} : I_K(\mathfrak{m})/(P_{K,1}(\mathfrak{m}) \cdot \mathrm{Nm}_{L/K} I_L(\mathfrak{m}) \xrightarrow{\sim} G\,.$$

Proof. Observe that, since $\mathfrak{m}$ is a modulus of definition for L/K, then $C_K(\mathfrak{m}) \subseteq \mathrm{Nm}_{L/K} C_L$. We claim that the isomorphism

$$C_K/C_K(\mathfrak{m}) \xrightarrow{\sim} Cl_K(\mathfrak{m})$$

from Proposition 6.1.5 restricts to an isomorphism

$$\mathrm{Nm}_{L/K} C_L/C_K(\mathfrak{m}) \xrightarrow{\sim} P_{K,1}(\mathfrak{m}) \cdot \mathrm{Nm}_{L/K} I_L(\mathfrak{m})/P_{K,1}(\mathfrak{m})\,.$$

Consider the modulus $\mathfrak{M} = \prod_{\mathfrak{P}} \mathfrak{P}^{\mathfrak{M}(\mathfrak{P})}$ of L, with $\mathfrak{M}(\mathfrak{P}) = e_{\mathfrak{P}|\mathfrak{p}}\mathfrak{m}(\mathfrak{p})$ if $\mathfrak{P}|\mathfrak{p}$. An easy application of the weak approximation theorem shows that $\mathbb{I}_L = L^\times \cdot \mathbb{I}_L(S(\mathfrak{M})) \cdot W_{\mathfrak{M}}$. Observe that $\mathrm{Nm}_{L/K} W_{\mathfrak{M}} \subseteq W_{\mathfrak{m}}$.

The isomorphism

$$C_K/C_K(\mathfrak{m}) \xrightarrow{\sim} Cl_K(\mathfrak{m})$$

is given by the chain of isomorphisms

$$C_K/C_K(\mathfrak{m}) \xrightarrow{\sim} \mathbb{I}_K/(K^\times \cdot W_{\mathfrak{m}}) \xrightarrow{\sim} \mathbb{I}_K(\mathfrak{m})/(P_{K,1}(\mathfrak{m}) \cdot W_{\mathfrak{m}}) \xrightarrow{\sim} Cl_K(\mathfrak{m})\,.$$

Applying this chain of isomorphisms to $\mathrm{Nm}_{L/K} C_L$, we get

$$\mathrm{Nm}_{L/K} C_L/C_K(\mathfrak{m}) \xrightarrow{\sim} K^\times \cdot \mathrm{Nm}_{L/K}\mathbb{I}_L/(K^\times \cdot W_{\mathfrak{m}}) = \mathrm{Nm}_{L/K}\mathbb{I}_L(S(\mathfrak{M})) \cdot K^\times \cdot W_{\mathfrak{m}}/(K^\times \cdot W_{\mathfrak{m}}) \xrightarrow{\sim}$$

$$\xrightarrow{\sim} \mathrm{Nm}_{L/K}\mathbb{I}_L(S(\mathfrak{M})) \cdot P_{K,1}(\mathfrak{m}) \cdot W_{\mathfrak{m}}/(P_{K,1}(\mathfrak{m}) \cdot W_{\mathfrak{m}}) \xrightarrow{\sim} \mathrm{Nm}_{L/K} I_L(\mathfrak{m})/P_{K,1}(\mathfrak{m})\,,$$

where for the last isomorphism we have used Lemma 4.2.2.

Now, since $\mathfrak{m}$ is a modulus of definition, from Proposition 6.1.8 we know that the diagram

$$\begin{array}{ccc} \mathbb{I}_K(\mathfrak{m})/(P_{K,1}(\mathfrak{m}) \cdot W_{\mathfrak{m}}) & & \\ \Big\downarrow \mathrm{id} & \searrow^{\phi_{L/K}} & \\ Cl_K(\mathfrak{m}) & \xrightarrow{\psi_{L/K}} & G \end{array}$$

is commutative. It is obvious that the map $\phi_{L/K}$ commutes with the isomorphisms

$$C_K/C_K(\mathfrak{m}) \xrightarrow{\sim} \mathbb{I}_K/(K^\times \cdot W_{\mathfrak{m}}) \xrightarrow{\sim} \mathbb{I}_K(\mathfrak{m})/(P_{K,1}(\mathfrak{m}) \cdot W_{\mathfrak{m}})\,,$$

so that we get the commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathrm{Nm}_{L/K}C_L/C_K(\mathfrak{m}) & \longrightarrow & C_K/C_K(\mathfrak{m}) & \xrightarrow{\phi_{L/K}} & G & \longrightarrow & 1 \\ & & \downarrow \simeq & & \downarrow \simeq & & \downarrow = & & \\ 1 & \longrightarrow & P_{K,1}(\mathfrak{m}) \cdot \mathrm{Nm}_{L/K} I_L(\mathfrak{m})/P_{K,1}(\mathfrak{m}) & \longrightarrow & Cl_K(\mathfrak{m}) & \xrightarrow{\psi_{L/K}} & G & \longrightarrow & 1 \end{array}$$

in which the vertical arrows are isomorphisms. Hence, since the first row is exact by the idelic Reciprocity Law (Theorem 5.1.3), so is the second, and the desired result follows. □

Definition 6.2.11. Let $\mathfrak{m}$ be a modulus of K. Then, the *ray class field for* $\mathfrak{m}$ is the finite Abelian extension $K_\mathfrak{m}$ of K corresponding, by the idelic Existence Theorem, to the subgroup $C_K(\mathfrak{m})$ of C_K.

Remark 33. Observe that, by Lemma 6.2.6, the modulus $\mathfrak{m}$ is a modulus of definition for $K_\mathfrak{m}/K$. By the idelic Reciprocity Law, the Galois group $\mathrm{Gal}(K_\mathfrak{m}/K)$ is isomorphic to the ray class group $Cl_K(\mathfrak{m}) \simeq C_K/C_K(\mathfrak{m})$. Therefore, we see that $\ker \psi_{L/K,S(\mathfrak{m})} = P_{K,1}(\mathfrak{m})$.

Remark 34. Let L be a finite Abelian extension of K. Then,

$$L \subseteq K_\mathfrak{m} \Leftrightarrow \mathrm{Nm}_{L/K}C_L \supseteq C_K(\mathfrak{m}) \Leftrightarrow \mathfrak{m} \text{ is a defining modulus for } L/K.$$

Thus, we can define the conductor of L/K as the smallest $\mathfrak{m}$ such that $L \subseteq K_\mathfrak{m}$.

Theorem 6.2.12. (Existence Theorem) Let $\mathfrak{m}$ be a modulus of K and let H be a congruence subgroup for $\mathfrak{m}$. Then, there exists a unique Abelian extension L of K such that all prime ideals of K which ramify in L divide $\mathfrak{m}$ and $\ker \psi_{L/K,S(\mathfrak{m})} = H$.

Proof. Let $K_\mathfrak{m}$ be the ray class field for $\mathfrak{m}$. Then, we have an isomorphism

$$\psi_{K_\mathfrak{m}/K,S(\mathfrak{m})} : I_K(\mathfrak{m})/P_{K,1}(\mathfrak{m}) \to \mathrm{Gal}(K_\mathfrak{m}/K)\,.$$

Let $L \subseteq K_\mathfrak{m}$ be the fixed field of $\psi_{K_\mathfrak{m}/K,S(\mathfrak{m})}(H/P_{K,1}(\mathfrak{m}))$. This is clearly a finite Abelian extension of K all of whose ramified primes divide $\mathfrak{m}$, and, since $\psi_{L/K,S(\mathfrak{m})}(\cdot) = \psi_{K_\mathfrak{m}/K,S(\mathfrak{m})}(\cdot)|_L$, we see that $\ker \psi_{L/K,S(\mathfrak{m})} = H$. The uniqueness part follows from Proposition 6.2.9. □

Definition 6.2.13. The *Hilbert class field* of K is the *ray class field* for the modulus $\mathfrak{m} = 1$.

It is clear that the *Hilbert class field* of a number field K is unramified over K. Moreover, we have the following result.

Theorem 6.2.14. The Hilbert class field of K is the maximal unramified Abelian extension of K (any other unramified Abelian extension of K is contained in the Hilbert class field).

Proof. Let L be the Hilbert class field of K and let M be any other unramified Abelian extension. Let M' be any finite subextension of M/K. Since it is unramified, the modulus $\mathfrak{m} = 1$ is a modulus of definition for M'/K. Therefore

$$\ker \psi_{L/K} = P_K \subseteq \ker \psi_{M'/K}\,,$$

which, by Proposition 6.2.9, implies that $M' \subseteq L$. Hence, we have $M \subseteq L$. □

Remark 35. For the Hilbert class field L of K, the Artin map $\psi_{L/K}$ gives an isomorphism

$$Cl_K = I_K/P_K \xrightarrow{\sim} \mathrm{Gal}(L/K)\,,$$

i.e. the Galois group of L/K is isomorphic to the ideal class group. As a consequence of this isomorphism, a prime ideal $\mathfrak{p}$ of K splits completely L if and only if it is principal.

Chapter 7

Applications

7.1 Kronecker-Weber theorem

References: [Cox13]

Lemma 7.1.1. Consider the number field $\mathbb{Q}$. Let m be a positive integer. The ray class field for $m\infty$ is $\mathbb{Q}(\zeta_m)$, where ζ_m denotes a primitive m-th root of unity.

Proof. The ray class field for $m\infty$ is the unique finite Abelian extension L of $\mathbb{Q}$ all of whose ramified primes divide $m\infty$ such that $\ker \psi_{L/\mathbb{Q},S(m\infty)} = P_{\mathbb{Q},1}(m\infty)$. We know that the primes of $\mathbb{Q}$ which ramify in $\mathbb{Q}(\zeta_m)$ must be among those dividing $m\infty$. Observe that any fractional ideal in $I_K(m\infty)$ can be written as $(a/b)\mathbb{Z}$, where a and b are positive integers relatively prime to m. For any prime $p \nmid m$, the Fröbenius element $(p, \mathbb{Q}(\zeta_m)/\mathbb{Q})$ is the $\mathbb{Q}$-automorphism mapping ζ_m to ζ_m^p. Therefore, the Artin map can be described as

$$\begin{aligned} \psi_{\mathbb{Q}(\zeta_m)/\mathbb{Q},S(m\infty)} : I_K(m\infty) &\to \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \simeq (\mathbb{Z}/m\mathbb{Z})^\times \\ \frac{a}{b}\mathbb{Z} &\mapsto [a][b]^{-1}. \end{aligned}$$

The kernel of this map is clearly the set of fractional ideals $(a/b)\mathbb{Z}$ with a and b positive integers relatively prime with m and such that $a \equiv b \pmod m$. But multiplying both a and b by an integer in $[a]^{-1}$, we can write this ideals with $a \equiv b \equiv 1 \pmod m$. Hence, we see that $\ker \psi_{\mathbb{Q}(\zeta_m)/\mathbb{Q},S(m\infty)} = P_{\mathbb{Q},1}(m\infty)$. □

Theorem 7.1.2. (Kronecker-Weber) Let L be a finite Abelian extension of $\mathbb{Q}$. Then L is contained in some cyclotomic extension $\mathbb{Q}(\zeta)$.

Proof. Let $\mathfrak{m}$ be a modulus of definition for L. We can assume that $\infty|\mathfrak{m}$, so that $\mathfrak{m} = m\infty$ for some integer m. Therefore, the extension L is contained in the ray class field $\mathbb{Q}_{m\infty} = \mathbb{Q}(\zeta_m)$, where ζ_m denotes a primitive m-th root of unity. □

7.2 Principal ideal theorem

References: [Neu99]

In this section, given a group G, we will use the notation G' rather than G^c to denote its commutator subgroup. The notation G'' will then refer to the commutator subgroup of G'.

Lemma 7.2.1. Let G be a group and let H be a subgroup of G of finite index. Then we have a commutative diagram

$$\begin{array}{ccc} G/G' & \xrightarrow{\text{Ver}} & H/H' \\ \downarrow \simeq & & \downarrow \simeq \\ I_G/I_G^2 & \xrightarrow{S} & (I_H + I_H I_G)/I_H I_G \end{array}$$

where the vertical arrows are induced by $\sigma \mapsto i_\sigma = \sigma - 1$ and the map S is given by

$$S(x \bmod I_G^2) = \sum_{s \in S} sx \bmod I_H I_G$$

for a system of representatives S of the right cosets of H in G such that $1 \in S$.

Proof. The fact that the first vertical arrow is an isomorphism was seen throughout the proof of Proposition 1.9.2. Let us check that the second vertical arrow is also an isomorphism. The elements $i_\sigma s$ with $\sigma \in H$, $\sigma \neq 1$ and $s \in S$, form a $\mathbb{Z}$-basis of $I_H + I_H I_G$: they generate $I_H + I_H I_G$ since they clearly generate I_H and for any $(\tau - 1)(\sigma s - 1)$ with $\tau, \sigma \in H$ and $s \in S$ we have the identity

$$(\tau - 1)(\sigma s - 1) = (\tau\sigma - 1)s - (\sigma - 1)s - (\tau - 1)\,, \tag{7.1}$$

and if $\sum_{\sigma,s} n_{\sigma,s} i_\sigma s = 0$ then

$$0 = \sum_{\sigma,s} n_{\sigma,s}(\sigma - 1)s = \sum_{\sigma,s} n_{\sigma,s}\sigma s - \sum_{\sigma,s} n_{\sigma,s} s\,,$$

whereby we deduce that all the coefficients $n_{\sigma,s}$ are zero because all the elements σs with $\sigma \in H$, $\sigma \neq 1$ and $s \in S$ together with the elements $s \in S$ are pairwise distinct. We can therefore define a map $I_H + I_H I_G \to H/H'$ by $i_\sigma s \mapsto \sigma \bmod H'$. Any $(\tau - 1)(\sigma s - 1) \in I_H I_G$ is mapped to $1 \bmod H'$ because of the identity (7.1). Hence we get a homomorphism $(I_H + I_H I_G)/I_H I_G$ which is clearly an inverse of the map in the diagram.

Now, take some $x \bmod G' \in G/G'$. For each $s \in S$, let $sx = x_s s'$ with $x_s \in H$ and $s' \in S$. Then, the image of $x \bmod G'$ by the transfer map is given by

$$\text{Ver}(x \bmod G') = \prod_{s \in S} x_s \bmod H'\,.$$

Going now downwards in the diagram we get

$$\sum_{s \in S} (x_s - 1) \bmod I_H I_G\,.$$

Going by the other way, we get

$$\sum_{s \in S} s(x - 1) \bmod I_H I_G\,,$$

and both expressions coincide because of the identities

$$(s - 1) + s(x - 1) = (x_s - 1) + (s' - 1) + (x_s - 1)(s' - 1)$$

together with the fact that the s' are all distict. □

Theorem 7.2.2. Let G be a finitely generated group. If G' has finite index in G, then the transfer map

$$\mathrm{Ver} : G/G' \to G'/G''$$

is the trivial homomorphism.

Proof. Replacing G by G/G'', we can assume that $G'' = \{1\}$ and hence that G' is Abelian. Let $S \ni 1$ be a set of representatives of the right cosets of G' in G, and let $g_1, \dots, g_n$ be a set of generators of G. Consider the homomorphism $\mathbb{Z}^n \to G/G'$ mapping each $e_j = (0, \dots, 0, 1, 0, \dots, 0)$ to g_j. This homomorphism is clearly surjective and, since G/G' is finite, its kernel has finite index in $\mathbb{Z}^n$, which means that the kernel has rank n and is therefore isomorphic to $\mathbb{Z}^n$. This provides an exact sequence

$$0 \longrightarrow \mathbb{Z}^n \xrightarrow{\ f\ } \mathbb{Z}^n \longrightarrow G/G' \longrightarrow 1$$

where f is given by a matrix $(m_{jk})_{1 \leqslant j,k \leqslant n}$ with integer coefficients and with $|\det(m_{jk})| = [G : G']$ (because the modulus of the determinant is the index of the image of f in $\mathbb{Z}^n$, which is the kernel of the surjective map $\mathbb{Z}^n \to G/G'$). In fact, we can obviously assume that $\det(m_{jk}) = [G : G']$

The image of each of the vectors e_k by f lies in the kernel of the map $\mathbb{Z}^n \to G/G'$, so that, for all k with $1 \leqslant k \leqslant n$, there is some $\tau_k \in G'$ such that

$$\tau_k \prod_{j=1}^{n} g_j^{m_{jk}} = 1\,.$$

Therefore, using the identity $i_{xy} = i_x + i_y + i_x i_y$ and taking into account that $\tau_k \in G'$, we deduce that there exist $\mu_{jk} \equiv m_{jk} \bmod I_G$ such that

$$\sum_{j=1}^{n} \mu_{jk} i_{g_j} = 0$$

for all k with $1 \leqslant k \leqslant n$. We can regard (μ_{jk}) as a matrix with coefficients in the commutative ring $\mathbb{Z}[G' \setminus G] \simeq \mathbb{Z}[G]/I_{G'}\mathbb{Z}[G]$. Define $\mu = \det(\mu_{jk})$, and let (λ_{jk}) be the adjoint matrix of (μ_{jk}). Then, we have

$$\mu i_{g_l} \equiv \sum_{j,k} \lambda_{kl}\mu_{jk} i_{g_j} = 0 \pmod{I_{G'}\mathbb{Z}[G]I_G}\,,$$

so that $\mu i_g \equiv 0 \mod I_{G'}\mathbb{Z}[G]I_G = I_{G'}I_G$ for all $g \in G$. Let $\mu = \sum_{s\in S} n_s \overline{s}$. Then, for all $\overline{g} \in G' \setminus G$,

$$\mu\overline{g} = \sum_{s\in S} n_s \overline{s}\,\overline{g} = \sum_{s\in S} n_s \overline{s}\,,$$

so we deduce that all the coefficients n_s are equal. Write $\mu = m\sum_{s\in S}\overline{s}$. We have

$$m[G : G'] \equiv \mu \equiv \det(m_{jk}) \equiv [G : G'] \pmod{I_G}\,,$$

so that $m = 1$. Finally, applying the previous lemma, the transfer map is trivial because

$$S(i_g \bmod I_G^2) = \sum_{s\in S} s i_g \equiv \mu i_g \equiv 0 \pmod{I_{G'}I_G}\,.$$

□

Let K be a number field. For a finite Galois extension M of K, not necessarily Abelian, we will write $\phi_{M/K}$ for the map $\phi_K(\cdot)|_L$, where L is the maximal Abelian subextension of M/K. For any prime v of K, we will write $\phi_{v,M/K}$ for $\phi_{v,L/K}$.

Lemma 7.2.3. Let E/K be a finite extension. Then, the diagram

$$\begin{array}{ccc} \mathbb{I}_K & \xrightarrow{\phi_K} & \mathrm{Gal}(K^{\mathrm{al}}/K)^{\mathrm{ab}} \\ \downarrow{\scriptstyle i} & & \downarrow{\scriptstyle \mathrm{Ver}} \\ \mathbb{I}_E & \xrightarrow{\phi_E} & \mathrm{Gal}(K^{\mathrm{al}}/E)^{\mathrm{ab}} \end{array}$$

commutes.

Proof. Let M be a Galois extension of K containing E. We claim that the diagram

$$\begin{array}{ccc} \mathbb{I}_K & \xrightarrow{\phi_{L/K}} & \mathrm{Gal}(M/K)^{\mathrm{ab}} \\ \downarrow{\scriptstyle i} & & \downarrow{\scriptstyle \mathrm{Ver}} \\ \mathbb{I}_E & \xrightarrow{\phi_{L/E}} & \mathrm{Gal}(M/E)^{\mathrm{ab}} \end{array}$$

commutes. Take any $(\alpha_u)_u \in \mathbb{I}_K$. Moving downwards and then to the right in the previous diagram we obtain

$$\prod_u \prod_{v|u} \phi_{v,M/E}(\alpha_u)\,.$$

Fix a prime u of K and a prime v of E dividing u. Let G_v be the decomposition group of v in E/K and let S be a system of representatives for the left cosets of G_v in $\mathrm{Gal}(E/K)$. For each prime τv of E, with $\tau \in S$, choose a prime $w_{\tau v}$ of M dividing τv (observe that the primes τv of E, with $\tau \in S$, are precisely the primes of E dividing u). For each $\sigma \in G_v$, choose an extension $\tilde{\sigma} \in \mathrm{Gal}(M_{w_v}/K_u)$, and, for each $\tau \in S$, choose an extension $\tau : M_{w_v} \to M_{w_{\tau v}}$. For each $\tau \in S$, the set $\tilde{G}_{\tau v}$ comprised of the elements $\tilde{\tau}\tilde{\sigma}\tilde{\tau}^{-1}$ with $\sigma \in G_v$ is a system of coset representatives of $\mathrm{Gal}(M_{w_{\tau v}}/E_{\tau v})$ in $\mathrm{Gal}(M_{w_{\tau v}}/K_u)$. Therefore, the transfer map from $\mathrm{Gal}(M_{w_{\tau v}}/K_u)$ to $\mathrm{Gal}(M_{w_{\tau v}}/E_{\tau v})$ is given by

$$\mathrm{Ver}(\rho \bmod \mathrm{Gal}(M_{w_{\tau v}}/K_u)') = \prod_{\sigma \in G_v} \tilde{\tau}\tilde{\sigma}\tilde{\tau}^{-1}\rho\varphi_{\tau v}(\tilde{\tau}\tilde{\sigma}\tilde{\tau}^{-1}\rho)^{-1}\,,$$

where for any $g \in \mathrm{Gal}(M_{w_{\tau v}}/K_u)$ the notation $\varphi_{\tau v}(g)$ stands for the element in $\tilde{G}_{\tau v}$ lying in the same coset as g. Let L be the maximal Abelian subextension of M/E. Using the second commutative diagram in Lemma 3.3.7, we get

$$\begin{aligned} \prod_{\tau \in S} \phi_{\tau v,M/E}(\alpha_u) = \prod_{\tau \in S} \phi_{M_{w_{\tau v}}/E_{\tau v}}(\alpha_u)|_L = \prod_{\tau \in S} \mathrm{Ver}(\phi_{M_{w_{\tau v}}/K_u}(\alpha_u))|_L = \\ = \prod_{\tau \in S} \prod_{\sigma \in G_v} \left(\tilde{\tau}\tilde{\sigma}\tilde{\tau}^{-1}\phi_{M_{w_{\tau v}}/K_u}(\alpha_u)\,\varphi_{\tau v}\left(\tilde{\tau}\tilde{\sigma}\tilde{\tau}^{-1}\phi_{M_{w_{\tau v}}/K_u}(\alpha_u)\right)^{-1}\right)|_L\,. \end{aligned}$$

Let $\phi_{M_{w_{\tau v}}/K_u}(\alpha_u)$ also denote any extension of this map to $\mathrm{Gal}(M_{w_{\tau v}}/K_u)$. Taking into account that we can assume

$$\phi_{M_{w_{\tau v}}/K_u}(\alpha_u) = \tilde{\tau}\phi_{M_{w_v}/K_u}(\alpha_u)\tilde{\tau}^{-1}$$

and the fact that the elements $\tilde{\tau}|_M\tilde{\sigma}|_M$ with $\tau \in S$ and $\sigma \in G_v$ form a system of representatives of the cosets of $\mathrm{Gal}(M/E)$ in $\mathrm{Gal}(M/K)$, we obtain

$$\begin{aligned}\prod_{\tau\in S}\phi_{\tau v,M/E}(\alpha_u) &= \prod_{\tau\in S}\prod_{\sigma\in G_v}\left(\tilde{\tau}\tilde{\sigma}\phi_{M_{w_v}/K_u}(\alpha_u)\tilde{\tau}^{-1}\,\varphi_{\tau v}\left(\tilde{\tau}\tilde{\sigma}\phi_{M_{w_v}/K_u}(\alpha_u)\tilde{\tau}^{-1}\right)^{-1}\right)|_L = \\ &= \prod_{\tau\in S}\prod_{\sigma\in G_v}\left(\tilde{\tau}\tilde{\sigma}\phi_{M_{w_v}/K_u}(\alpha_u)\,\varphi_v\left(\tilde{\sigma}\phi_{M_{w_v}/K_u}(\alpha_u)\right)^{-1}\tilde{\tau}^{-1}\right)|_L = \\ &= \prod_{\tau\in S}\prod_{\sigma\in G_v}\left(\tilde{\tau}|_M\,\tilde{\sigma}|_M\,\phi_{u,M/K}(\alpha_u)\,\varphi\left(\tilde{\sigma}|_M\,\phi_{u,M/K}(\alpha_u)\right)^{-1}\tilde{\tau}|_M^{-1}\right)|_L = \mathrm{Ver}(\phi_{u,M/K})\,,\end{aligned}$$

where the transfer map is from $\mathrm{Gal}(M/K)$ to $\mathrm{Gal}(M/E)$ and for $g \in \mathrm{Gal}(M/K)$, $\varphi(g)$ denotes the corresponding representative among the elements $\tilde{\tau}|_M\tilde{\sigma}|_M$ with $\tau \in S$ and $\sigma \in G_v$. For the last equality we have used that $\mathrm{Gal}(M/E)$ is a normal subgroup of $\mathrm{Gal}(M/K)$ because E/K is a Galois extension.

The diagram in the statement is obtained by taking projective limits. □

Theorem 7.2.4. (Principal ideal theorem) Let L be the Hilbert class field of K and let $\mathcal{O}_L$ be its ring of integers. Then, every ideal $\mathfrak{a}$ of K becomes principal in the Hilbert class field (i.e. the ideal $\mathfrak{a}\mathcal{O}_L$ is principal).

Proof. Let L' be the Hilbert class field of L. For every K-embedding $\sigma : L' \hookrightarrow \mathbb{C}$, we have $\sigma L = L$ because L/K is a Galois extension. Therefore $\tau L'$ is the Hilbert class field of $\tau L = L$, so that $\tau L' = L'$. This shows that L'/K is a Galois extension.

Consider the diagram

$$\begin{array}{ccccc} I_K/P_K & \xrightarrow{\simeq} & C_K/\mathrm{Nm}_{L'/K}C_{L'} & \xrightarrow{\phi_{L'/K}} & \mathrm{Gal}(L'/K)^{\mathrm{ab}} \\ \downarrow{\scriptstyle \mathfrak{a}\mapsto\mathfrak{a}\mathcal{O}_L} & & \downarrow{\scriptstyle i} & & \downarrow{\scriptstyle \mathrm{Ver}} \\ I_L/P_L & \xrightarrow{\simeq} & C_L/\mathrm{Nm}_{L'/L}C_{L'} & \xrightarrow{\phi_{L'/L}} & \mathrm{Gal}(L'/L)^{\mathrm{ab}} \end{array},$$

where all the horizontal arrows are isomorphisms. The first square trivially commutes and the second square commutes because of the previous lemma. On the other hand, observe that L' is unramified over L, which in turn is unramified over L. This implies that L' is unramified over K. Then, since L is the maximal unramified Abelian extension of K, it is the maximal Abelian subextension of L'/K. This means that $\mathrm{Gal}(L'/L)$ is the commutator subgroup of $\mathrm{Gal}(L'/K)$. Hence, by Theorem 7.2.2, the last vertical arrow in the previous diagram is the trivial homomorphism, so that we deduce that so is the first vertical arrow, and the desired result follows. □

7.3 Primes of the form $x^2 + ny^2$

References: [Cox13]

Let $\mathcal{O}$ be an order in a quadratic field K. Let f be the conductor of $\mathcal{O}$. Then, we have the inclusions

$$P_{K,1}(f) \subseteq P_{K,\mathbb{Z}}(f) \subseteq I_K(f)\,,$$

which show that $P_{K,\mathbb{Z}}(f)$ is a congruence subgroup for the modulus f and through the isomorphism $Cl(\mathcal{O}) \simeq I_K(f)/P_{K,\mathbb{Z}}(f)$, the group $Cl(\mathcal{O})$ can be viewed as a generalized ideal class group

for f. In particular, we deduce that $Cl(\mathcal{O})$ is a finite group. Its order is often referred to as the *class number of* $\mathcal{O}$ and will be denoted by $h(\mathcal{O})$. Since an order in a quadratic field is uniquely determined by its discriminant D, we will also write $h(D)$ to denote the class number.

According to the Existence Theorem (Theorem 6.2.12), there exists a unique Abelian extension L of K such that all primes of K ramifying in L divide f and $\ker \psi_{L/K,S(f)} = P_{K,\mathbb{Z}}(f)$. This extension is the *ring class field of* $\mathcal{O}$. If $\mathcal{O} = \mathcal{O}_K$, it is clear that this is in fact the Hilbert class field of K.

Remark 36. For the ring class field L of $\mathcal{O}$, the Artin map $\psi_{L/K,S(f)}$ induces an isomorphism

$$Cl(\mathcal{O}) \simeq I_K(f)/P_{K,\mathbb{Z}}(f) \xrightarrow{\simeq} \mathrm{Gal}(L/K)$$

which shows that $[L : K] = h(\mathcal{O})$.

Lemma 7.3.1. Let K be an imaginary quadratic field and let L/K be a finite Galois extension. Let τ stand for complex conjugation. Then, L is Galois over $\mathbb{Q}$ if and only it $\tau(L) = L$.

Proof. First, assume that L is Galois over $\mathbb{Q}$. Then, any $\mathbb{Q}$-embedding of L into $\mathbb{C}$ has image L, and, in particular, $\tau(L) = L$. For the converse implication, assume that $\tau(L) = L$. Then, since $\tau \notin \mathrm{Gal}(L/K)$ (because K is an imaginary quadratic field) we see that the group of $\mathbb{Q}$-automorphisms of L has at least order $2[L : K]$, and the result follows. □

Lemma 7.3.2. Let $\mathcal{O}$ be an order in an imaginary quadratic field K and let L be its ring class field. Then L is a Galois extension of $\mathbb{Q}$ and

$$\mathrm{Gal}(L/\mathbb{Q}) \simeq \mathrm{Gal}(L/K) \rtimes (\mathbb{Z}/2\mathbb{Z})$$

with the action of the non-trivial element of $(\mathbb{Z}/2\mathbb{Z})$ on $\mathrm{Gal}(L/K)$ defined by $\sigma \mapsto \sigma^{-1}$.

Proof. Let f be the conductor of $\mathcal{O}$. Let τ denote complex conjugation. Observe that $\tau(w_K) = d_K - w_K \in \mathcal{O}_K$, so that $\tau(\mathcal{O}_K) = \mathcal{O}_K$ and clearly $\tau(P_{K,\mathbb{Z}}(f)) = P_{K,\mathbb{Z}}(f)$. On the other hand, from the fact that for any prime ideal $\mathfrak{p}$ of K we have $\tau(\mathfrak{p}, L/K)\tau^{-1} = (\tau\mathfrak{p}, \tau(L)/K)$ we deduce that $\ker \psi_{\tau(L)/K,S(f)} = \tau(\ker \psi_{L/K,S(f)})$. Altogether, we get

$$\ker \psi_{\tau(L)/K,S(f)} = \tau(\ker \psi_{L/K,S(f)}) = \tau(P_{K,\mathbb{Z}}(f)) = P_{K,\mathbb{Z}}(f) = \ker \psi_{L/K,S(f)}$$

and the uniqueness part of the Existence Theorem implies $\tau(L) = L$. Then, by the previous lemma, L is a Galois extension of $\mathbb{Q}$.

Since $\tau \in \mathrm{Gal}(L/\mathbb{Q})$, the exact sequence

$$1 \longrightarrow \mathrm{Gal}(L/K) \longrightarrow \mathrm{Gal}(L/\mathbb{Q}) \longrightarrow \mathrm{Gal}(K/\mathbb{Q}) \longrightarrow 0$$

is split, so that we get an isomorphism

$$\mathrm{Gal}(L/K\mathbb{Q}) \simeq \mathrm{Gal}(L/K) \rtimes \mathrm{Gal}(K/\mathbb{Q}) \simeq \mathrm{Gal}(L/K) \rtimes (\mathbb{Z}/2\mathbb{Z})$$

with the action of the non-trivial element of $(\mathbb{Z}/2\mathbb{Z})$ on $\mathrm{Gal}(L/K)$ given by $\sigma \mapsto \tau\sigma\tau^{-1}$. Since for all prime ideal $\mathfrak{p}$ of K it holds $\tau(\mathfrak{p}, L/K)\tau^{-1} = (\tau\mathfrak{p}, \tau(L)/K) = (\tau\mathfrak{p}, L/K)$, this action corresponds through the isomorphism $I_K(f)/P_{K,\mathbb{Z}}(f) \simeq \mathrm{Gal}(L/K)$ to an action on $I_K(f)/P_{K,\mathbb{Z}}(f)$ induced by $\mathfrak{a} \mapsto \tau\mathfrak{a}$. But for any (integral) ideal $\mathfrak{a}$ we have $\mathfrak{a} \cdot \tau\mathfrak{a} = N(\mathfrak{a})\mathcal{O}_K$ (see Lemma B.0.9), which shows that the map $\mathfrak{a} \mapsto \tau\mathfrak{a}$ sends any element in $I_K(f)/P_{K,\mathbb{Z}}(f)$ to its inverse, and then returning to $\mathrm{Gal}(L/K)$ we get the desired result. □

For any ideal $\mathfrak{a}$ of $\mathcal{O}_K$, we will use the notation $\overline{\mathfrak{a}}$ for complex conjugation.

Proposition 7.3.3. Let $n > 0$ be a positive integer. Let K be the quadratic number field $\mathbb{Q}(\sqrt{-n})$, and let L be the ring class field of the order $\mathbb{Z}[\sqrt{-n}]$ in K. Then, in order that an odd prime p not dividing n be of the form $x^2 + ny^2$, with $x, y \in \mathbb{Z}$, it is necessary and sufficient that it split completely in L.

Proof. Let $\mathcal{O} = \mathbb{Z}[\sqrt{-n}]$ and let f be the conductor of $\mathcal{O}$. Let $D = -4n$ be the discriminant of the order $\mathcal{O}$. Then $-4n = f^2 d_K$, so that an odd prime not dividing n does not divide d_K and is therefore unramified in K. It is also unramified in L, since p does not divide f and therefore neither do the ideals of K above p.

We will now prove the statement by proving, for any odd prime p not dividing n, the following chain of equivalences:

$$\begin{aligned} p \text{ is of the form } x^2 + ny^2 &\iff p\mathcal{O}_K = \mathfrak{p}\overline{\mathfrak{p}}, \text{ with } \mathfrak{p} \neq \overline{\mathfrak{p}} \text{ and } \mathfrak{p} = \alpha\mathcal{O}_K \text{ with } \alpha \in \mathcal{O} \\ &\iff p\mathcal{O}_K = \mathfrak{p}\overline{\mathfrak{p}}, \text{ with } \mathfrak{p} \neq \overline{\mathfrak{p}} \text{ and } \mathfrak{p} \in P_{K,\mathbb{Z}}(f) \\ &\iff p\mathcal{O}_K = \mathfrak{p}\overline{\mathfrak{p}}, \text{ with } \mathfrak{p} \neq \overline{\mathfrak{p}} \text{ and } (\mathfrak{p}, L/K) = 1 \\ &\iff p \text{ splits completely in } L. \end{aligned}$$

For the first equivalence, assume that $p = x^2 + ny^2$. Then taking $\alpha = x + y\sqrt{-n}$ and $\mathfrak{p} = \alpha\mathcal{O}_K$, we clearly have that $\alpha \in \mathcal{O}$ and $p\mathcal{O}_K = \mathfrak{p}\overline{\mathfrak{p}}$, with $\mathfrak{p} \neq \overline{\mathfrak{p}}$ because p does not ramify in $\mathcal{O}_K$. Conversely, assume that $p = \mathfrak{p}\overline{\mathfrak{p}}$ with $\mathfrak{p} = \alpha\mathcal{O}_K$ for some $\alpha = x+y\sqrt{-n} \in \mathcal{O}$. Then, clearly $p\mathcal{O}_K = (x+y\sqrt{-n})(x-y\sqrt{-n})\mathcal{O}_K = (x^2+ny^2)\mathcal{O}_K$ and $p = x^2+ny^2$. The second equivalence follows from the equivalence (B.1). The third equivalence follows from the isomorphism $I_K(f)/P_{K,\mathbb{Z}}(f) \simeq \mathrm{Gal}(L/K)$ provided by the Artin map $\psi_{L/K,S(f)}$. For the final equivalence, observe that the condition $(\mathfrak{p}, L/K) = 1$ is equivalent to the fact that $\mathfrak{p}$ split completely in L. □

Lemma 7.3.4. Let K be an imaginary quadratic field and let L be a finite extension of K which is also Galois over $\mathbb{Q}$. Then, for any $\alpha \in L \cap \mathbb{R}$,

$$L \cap \mathbb{R} = \mathbb{Q}(\alpha) \iff L = K(\alpha)\,.$$

Proof. Let τ denote complex conjugation. Since L is Galois over $\mathbb{Q}$, then, by Lemma 7.3.1, we know that $\tau(L) = L$. The subfield of L fixed by τ is clearly $L \cap \mathbb{R}$; therefore, we deduce that $[L : L \cap \mathbb{R}] = 2$. Thus, since we also have $[K : \mathbb{Q}] = 2$, we see that $[L \cap \mathbb{R} : \mathbb{Q}] = [L : K]$.

Now, for any $\alpha \in L \cap \mathbb{R}$, observe that $\mathbb{Q}(\alpha) \neq K(\alpha)$, because clearly $\mathbb{Q}(\alpha) \subseteq \mathbb{R}$. Then, since $[K(\alpha) : \mathbb{Q}(\alpha)] \leqslant [K : \mathbb{Q}] = 2$, necessarily $[K(\alpha) : \mathbb{Q}(\alpha)] = 2$, whereby we deduce that $[\mathbb{Q}(\alpha) : \mathbb{Q}] = [K(\alpha) : K]$. This fact, combined with the equality $[L \cap \mathbb{R} : \mathbb{Q}] = [L : K]$, clearly implies the lemma. □

Remark 37. In the conditions of the previous lemma, there always exists a real algebraic integer α such that $L = K(\alpha)$ (we need simply take some algebraic integer $\alpha \in \mathcal{O}_L \cap \mathbb{R}$ such that $\mathbb{Q}(\alpha) = L \cap \mathbb{R}$, which exists because of the primitive element theorem).

Proposition 7.3.5. Let K be an imaginary quadratic field and let L be a finite extension of K which is Galois over $\mathbb{Q}$. Let $\alpha \in \mathcal{O}_L \cap \mathbb{R}$ be such that $L = K(\alpha)$, and let $f(X) \in \mathbb{Z}[X]$ be its minimal polynomial over $\mathbb{Q}$. Then, for any prime p not dividing the discriminant of $f(X)$,

$$p \text{ splits completely in L} \iff \begin{cases} (d_K/p) = 1 \text{ and there is an integer solution} \\ \text{to the congruence } f(X) \equiv 0 \pmod{p} \end{cases}$$

Proof. Observe that, since $[L \cap \mathbb{R} : \mathbb{Q}] = [L : K]$, we have that $f(X)$ is also the minimal polynomial of α over K. If a prime p splits completely in L, then it clearly splits completely in K and hence $(d_K/p) = 1$. Therefore, we may prove the equivalence assuming that $(d_K/p) = 1$ (i.e. that p splits completely in K). So let p be a prime not dividing the discriminant of $f(X)$ and with $(d_K/p) = 1$, and let $p\mathcal{O}_K = \mathfrak{p}\overline{\mathfrak{p}}$ be its factorization in prime ideals in $\mathcal{O}_K$. Then we have $\mathcal{O}_K/\mathfrak{p} \simeq \mathbb{Z}/p\mathbb{Z}$. Since p does not divide the discriminant of $f(X)$, we have that $f(X)$ is separable modulo $\mathfrak{p}$, so that we get

$$\begin{aligned} p \text{ splits completely in } L &\iff f(X) \equiv 0 \pmod{\mathfrak{p}} \text{ has a solution in } \mathcal{O}_K \\ &\iff f(X) \equiv 0 \pmod{p} \text{ has a solution in } \mathbb{Z}. \end{aligned}$$

□

We know that the Artin map for the ring class field L of an order $\mathcal{O}$ in an imaginary quadratic field K induces an isomorphism between the ideal class group $Cl(\mathcal{O})$ and the Galois group $\mathrm{Gal}(L/K)$. Let D be the discriminant of $\mathcal{O}$. Then, if in the previous proposition we take L to be the ring class field of $\mathcal{O}$, the degree of the polynomial $f(X)$ is $[L : K] = h(D)$.

Combining Proposition 7.3.3 and Proposition 7.3.5, we get the following theorem:

Theorem 7.3.6. Let n be a positive integer. Then, there exists a monic irreducible polynomial $f_n(X)$ of degree $h(-4n)$ such that, for any prime p not dividing neither n nor the discriminant of $f_n(X)$,

$$p \text{ is of the form } x^2 + ny^2 \iff \begin{cases} (-n/p) = 1 \text{ and there is an integer solution} \\ \text{to the congruence } f_n(X) \equiv 0 \pmod{p}. \end{cases}$$

Moreover, if L is the ring class field of the order $\mathbb{Z}[\sqrt{-n}]$, then the polynomial $f_n(X)$ can be taken to be the minimal polynomial of any $\alpha \in \mathcal{O}_L \cap \mathbb{R}$ such that $L \cap \mathbb{R} = \mathbb{Q}(\alpha)$ (or equivalently such that $L = K(\alpha)$, with $K = \mathbb{Q}(\sqrt{-n})$).

Appendix A

Kummer theory

References: [Mil17b], [Mil13]

Let K be a field containing a primitive n-th root of unity ζ, with $n \geqslant 2$. Assume, moreover, that the characteristic of K does not divide n.

Proposition A.0.1. Under the previous conditions:

1. Every cyclic extension L/K of degree n is of the form $L = K(\alpha)$ for some α satisfying $\alpha^n \in K$.
2. If α is a root of $X^n - a \in K[X]$, then $K(\alpha)/K$ is cyclic of degree the minimum positive integer m such that $\alpha^m \in K$, and such m is always a divisor of n.

Proposition A.0.2. Let $K\left(a^{1/n}\right)$ and $K\left(b^{1/n}\right)$ be two cyclic extensions of degree n within the same algebraic closure of K. Then,

$$K\left(a^{1/n}\right) = K\left(b^{1/n}\right) \iff \langle a\rangle K^{\times n}/K^{\times n} = \langle b\rangle K^{\times n}/K^{\times n}\,.$$

Proof. The condition on the right (i.e. that a and b generate the same subgroup in $K^\times/K^{\times n}$) is equivalent to the fact that $b = a^r c^n$ for some $c \in K^\times$ and some r such that $(r, n) = 1$. Then, the implication from right to left is easy.

For the converse, assume that $K(\alpha) = K(\beta)$, where $\alpha^n = a$, $\beta^n = b$ and no lower positive power of neither α nor β belongs to K. Let $L = K(\alpha) = K(\beta)$, and let $G = \mathrm{Gal}(L/K) = \langle\sigma\rangle$. The elements $\tau \in G$ map α to another root of $X^n - a$, i.e to $\zeta^i\alpha$ for some i, and we have such an element $\tau \in G$ for each $i \pmod n$, so that, since σ is a generator of G, it maps α to $\zeta^i\alpha$ for some primitive n-th root ζ^i. We may assume $i = 1$. The same argument shows that $\sigma\beta = \zeta^r\beta$ for some primitive n-th root ζ^r, i.e. for some r such that $(r, n) = 1$.

Since the elements $1, \alpha, \ldots, \alpha^{n-1}$ for a K-basis of L, we can write

$$\beta = \sum_{i=0}^{n-1} x_i\alpha^i$$

for some $x_i \in K$. Applying σ on each side, and using the way in which σ acts on α and on β, we get:

$$\zeta^r\beta = \sum_{i=0}^{n-1} x_i\zeta^i\alpha^i$$

so that, replacing β by its expression in terms of the powers of α and equating the coresponding coefficients, we get

$$\zeta^r x_i = \zeta^i x_i \text{ for all } i \in \{0, 1, \ldots, n-1\}.$$

Thus, $x_i = 0$ for all $i \neq r$, so that $\beta = x_r \alpha^r$ and $b = a^r x_r^n$. □

Lemma A.0.3. Let L/K be a finite Galois extension with Galois group $G = \mathrm{Gal}(L/K)$. Then, there is an isomorphism

$$\left(K^\times \cap L^{\times n}\right) / K^{\times n} \simeq \mathrm{Hom}(G, \mu_n)\,.$$

Consequently, in the particular case in which G is Abelian of exponent a divisor of n, we get:

$$[K^\times \cap L^{\times n} : K^{\times n}] = |G|\,.$$

Proof. We have the exact sequence of G-modules

$$1 \longrightarrow \mu_n \longrightarrow L^\times \xrightarrow{x \mapsto x^n} L^{\times n} \longrightarrow 1\,,$$

from which we obtain a long exact sequence in cohomology. Taking into account that, because of Hilbert's theorem 90, we have $H^1(G, L^\times) = 1$, the first part of the long exact sequence reads

$$1 \longrightarrow \mu_n \longrightarrow K^\times \xrightarrow{x \mapsto x^n} K^\times \cap L^{\times n} \longrightarrow H^1(G, \mu_n) \longrightarrow 1\,.$$

Since G acts trivially on μ_n, we have $H^1(G, \mu_n) \simeq \mathrm{Hom}(G, \mu_n)$, so that we get the desired isomorphism from the previous exact sequence:

$$\begin{aligned} \left(K^\times \cap L^{\times n}\right) / K^{\times n} &\to \mathrm{Hom}(G, \mu_n) \\ aK^\times &\mapsto \left[\sigma \mapsto \frac{\sigma a^{1/n}}{a^{1/n}}\right]. \end{aligned}$$

If G is Abelian with exponent a divisor of n, $\mathrm{Hom}(G, \mu_n)$ is the dual of G, i.e. the group comprised of all characters $\chi : G \to \mathbb{C}^\times$, so that $|\mathrm{Hom}(G, \mu_n)| = |G|$ and then the previous isomorphism implies

$$[K^\times \cap L^{\times n} : K^{\times n}] = |G|\,.$$

□

Proposition A.0.4. There is a bijection between the finite Abelian extensions of K with exponent a divisor of n contained in a certain algebraic closure of K and the subgroups of $K^\times$ which contain $K^{\times n}$ as a subgroup of finite index, which is given by the map

$$L \to K^\times \cap L^{\times n}$$

with inverse

$$B \mapsto K(B^{1/n})\,.$$

Proof. Let L be a finite Abelian extension of K with exponent a divisor of n. Let us define $B(L) = K^\times \cap L^{\times n}$. Then, the inclusion $K(B(L)^{1/n}) \subseteq L$ is clear, and also is, for any subgroup B of $K^\times$, the inclusion $B \subseteq B(K(B^{1/n}))$. Taking into account these inclusions, we get

$$[L:K] \geqslant [K(B(L)^{1/n}):K] = [B(K(B(L)^{1/n})):K^{\times n}] \geqslant [B(L):K^{\times n}]\,,$$

where the equality in the middle follows from the previous lemma. Also from the previous lemma we have $[L:K] = [B(L):K^{\times n}]$, so all the previous inequalities are actually equalities and, from the first one, $L = K(B(L)^{1/n})$.

Now let B a subgroup of $K^\times$ which contains $K^{\times n}$ as a subgroup of finite index, and define $L = K(B^{1/n})$. Since $[B:K^{\times n}]$ is finite, there is a finite set S of generators of $B/K^{\times n}$, and we can write

$$L = \prod_{a\in S} K(a^{1/n})\,.$$

Then L is clearly a finite Galois extension. Let $G = \mathrm{Gal}(L/K)$. We claim that L/K is an Abelian extension. To see it, take into account that any $\sigma \in G$ is fully determined by its action on $S^{1/n}$, and, for each $a \in S$, it must satisfy $\sigma a^{1/n} = \zeta^{i_{\sigma,a}} a^{1/n}$ for some integer $i_{\sigma,a}$. Then, given $\sigma_1, \sigma_2 \in G$, it is immediate to check that $\sigma_1\sigma_2 a^{1/n} = \sigma_2\sigma_1 a^{1/n}$ for all $a \in S$, and so $\sigma_1\sigma_2 = \sigma_2\sigma_1$. Moreover, it is clear that G has exponent a divisor of n.

Taking into account the previous lemma, we have the isomorphism

$$\begin{aligned} B(L)/K^{\times n} &\to \mathrm{Hom}(G,\mu_n) \\ aK^\times &\mapsto \left[\sigma \mapsto \frac{\sigma a^{1/n}}{a^{1/n}}\right]. \end{aligned}$$

Since G has exponent a divisor of n, $\mathrm{Hom}(G,\mu_n)$ is the dual of the finite Abelian group G, so that $\mathrm{Hom}(G,\mu_n) \simeq G$. For each subgroup $H \subseteq G$, we may naturally indentify $\mathrm{Hom}(G/H,\mu_n)$ with the subgroup of $\mathrm{Hom}(G,\mu_n)$ comprised of those characters χ such that $\chi(h) = 1$ for all $h \in H$. All these are clearly different subgroups of $\mathrm{Hom}(G,\mu_n)$, and they are in fact all the subgroups of $\mathrm{Hom}(G,\mu_n)$ because of the isomorphism $\mathrm{Hom}(G,\mu_n) \simeq G$.

Hence, under the isomorphism

$$B(L)/K^{\times n} \to \mathrm{Hom}(G,\mu_n)\,,$$

we see that $B/K^{\times n}$ is mapped to $\mathrm{Hom}\,(G/H,\mu_n)$, where H is the subgroup of G comprised of those σ such that $\sigma a^{1/n} = a^{1/n}$ for all $a \in B$. But, since $L = K(B^{1/n})$, such a σ can only be the identity, so that the image of $B/K^{\times n}$ is $\mathrm{Hom}(G,\mu_n)$ and, consequently, $B = B(L) = B(K(B^{1/n}))$. □

Proposition A.0.5. Let K be a number field containing a primitive n-th root of unity ζ, and let $L = K(a_1^{1/n},\ldots,a_m^{1/n})$ with $a_i \in \mathcal{O}_K$ for all i. Then, for any finite prime v of K, if na_i is a unit in K_v, then v is unramified in L.

Proof. Since $L = \prod_{i=1}^m K(a_i^{1/n})$, a finite prime v of K is unramified in L if and only if it is unramified in $K(a_i^{1/n})$ for all i, so we need only prove the proposition for the case $L = K(a^{1/n})$, $a \in \mathcal{O}_K$.

Take α such that $\alpha^n = a$, and let $d|n$ be the degree of the extension $K(\alpha)/K$, which is the minimum positive integer k satisfying that $\alpha^k \in K$. Then, the minimal polynomial of α is $f(X) = X^d - a$, and we have

$$\begin{aligned} \mathrm{disc}(f) &= (-1)^{\frac{d(d-1)}{2}} \mathrm{Nm}_{L/K} f'(\alpha) = (-1)^{\frac{d(d-1)}{2}} \mathrm{Nm}_{L/K}(d\alpha^{d-1}) = \\ &= (-1)^{\frac{d(d-1)}{2}} (-1)^{(d+1)(d-1)} d^d a^{d-1}\,. \end{aligned}$$

Then, if v does not divide na, it does not divide $\mathrm{disc}(f)$ and, consequently, neither it divides $\mathrm{disc}(\mathcal{O}_L/\mathcal{O}_K)$, which implies that v is unramified in L. □

Appendix B

Orders in quadratic number fields

References: [Cox13], [Neu99], [Sam70]

Throughout this chapter, K will denote a number field of degree n over $\mathbb{Q}$. We will denote its ring of integers by $\mathcal{O}_K$ and its discriminant by d_K.

Definition B.0.1. Let K be a number field. An *order* in K is a subring $\mathcal{O} \subseteq \mathcal{O}_K$ which contains a $\mathbb{Q}$-basis of K.

It is clear that $\mathbb{Z} \subseteq \mathcal{O}$ for any order $\mathcal{O}$ in K, so $\mathcal{O}$ may be regarded as a $\mathbb{Z}$-module. Therefore, since $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank n, and $\mathcal{O}$ is a submodule of $\mathcal{O}_K$ which contains a $\mathbb{Q}$-basis of K, we deduce that $\mathcal{O}$ is also a free $\mathbb{Z}$-module of rank n. Because of this, we also see that $\mathcal{O}$ has finite index in $\mathcal{O}_K$.

Another point is that K is the field of fractions of $\mathcal{O}$. This follows because, setting m to be the index of $\mathcal{O}$ in $\mathcal{O}_K$, we have that $m\mathcal{O}_K \subseteq \mathcal{O}$, so that, since K is the field of fractions of $\mathcal{O}_K$, it is also the field of fractions of $\mathcal{O}$.

Proposition B.0.2. An order $\mathcal{O}$ in K is a Noetherian ring and every prime ideal of $\mathcal{O}$ is maximal.

Proof. Since $\mathcal{O}$ is a finitely generated $\mathbb{Z}$-module, every $\mathbb{Z}$-submodule is also finitely generated. In particular, any ideal of $\mathcal{O}$ is finitely generated as a $\mathbb{Z}$-module and, *a fortiori*, as an $\mathcal{O}$-module. This shows that $\mathcal{O}$ is a Noetherian ring.

Now, let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}$. Take some $x \in \mathfrak{p}$. Since $x \in \mathcal{O} \subseteq \mathcal{O}_K$, it is integral over $\mathbb{Z}$, so that

$$x^r + a_{r-1}x^{r-1} + \cdots a_1 x + a_0 = 0\,,$$

for some $r > 0$ and some $a_0, a_1, \ldots, a_{r-1} \in \mathbb{Z}$. We may obviously assume that $a_0 \neq 0$. We have $a_0 \in \mathfrak{p} \cap \mathbb{Z}$, so that $a_0\mathcal{O} \subseteq \mathfrak{p} \subseteq \mathcal{O}$ and, consequently, the quotient $\mathcal{O}/\mathfrak{p}$ is finite. Then, this quotient is a finite integral domain, which implies that it is a field and therefore that $\mathfrak{p}$ is a maximal ideal. □

Note that, unless $\mathcal{O} = \mathcal{O}_K$, an order $\mathcal{O}$ is not integrally closed, and consequently it is not a Dedekind domain.

Definition B.0.3. The *conductor* of an order $\mathcal{O}$ in K is the biggest ideal $\mathfrak{f}$ of $\mathcal{O}_K$ contained in $\mathcal{O}$, that is:

$$\mathfrak{f} = \{a \in \mathcal{O}_K : a\mathcal{O}_K \subseteq \mathcal{O}\}\,.$$

Remark 38. Since $\mathcal{O}_K$ is finitely generated as a $\mathbb{Z}$-module and $\mathcal{O}$ contains a $\mathbb{Q}$-basis of K, it follows easily that $\mathfrak{f} \neq 0$.

From now on, we set $n = 2$. The results which we present are specific for orders in quadratic number fields. In this case, defining

$$w_K = \frac{d_K + \sqrt{d_K}}{2},$$

we know that $\mathcal{O}_K = \mathbb{Z}\langle 1, w_K \rangle$.

Lemma B.0.4. Let $\mathcal{O}$ be an order in K and let $f = [\mathcal{O}_K : \mathcal{O}]$. Then,

$$\mathcal{O} = \mathbb{Z}\langle 1, f w_K \rangle .$$

Proof. We have $f\mathcal{O}_K \subseteq \mathcal{O}$, so that $\mathbb{Z} + f\mathcal{O}_K \subseteq \mathcal{O}$. But $\mathbb{Z} + f\mathcal{O}_K = \mathbb{Z} + f\mathbb{Z}[1, w_K] = \mathbb{Z}\langle 1, f w_K \rangle$, so that in fact we get $\mathbb{Z}\langle 1, f w_K \rangle \subseteq \mathcal{O}$, and, since both $\mathbb{Z}\langle 1, f w_K \rangle$ and $\mathcal{O}$ have index f in $\mathcal{O}_K$, they must be equal. □

Lemma B.0.5. Let $\mathcal{O}$ be an order in K and let $f = [\mathcal{O}_K : \mathcal{O}]$. Then $f\mathcal{O}_K$ is the conductor of $\mathcal{O}$.

Proof. Since $\mathcal{O}_K = \mathbb{Z}\langle 1, w_K \rangle$, in order that $\alpha = a + b w_K \in \mathcal{O}_K$, with $a, b \in \mathbb{Z}$, be in the conductor $\mathfrak{f}$ of $\mathcal{O}$ it is necesary and sufficient that both $\alpha \cdot 1$ and $\alpha \cdot w_K$ be in $\mathcal{O}_K$. Observe that

$$\begin{aligned} \alpha \cdot 1 &= a + b w_K \\ \alpha w_K &= (a + b w_K) w_K = b \frac{d_k(1 - d_k)}{4} + (a + b d_K) w_K , \end{aligned}$$

so that, by the previous lemma, these conditions are equivalent to the condition $f \mid a$ and $f \mid b$, i.e. to the condition $\alpha \in f\mathcal{O}_K$. □

Remark 39. Because of this last result, we will also refer to $f = [\mathcal{O}_K : \mathcal{O}]$ as the conductor of the order $\mathcal{O}$.

Remark 40. If $\mathcal{O}$ is an order in K and $f = [\mathcal{O}_K : \mathcal{O}]$, then the discriminant of $\mathcal{O}$ as a $\mathbb{Z}$-module, to which we will simply refer as the *discriminant of* $\mathcal{O}$, is $D = f^2 d_K$. Consequently, we see that $K = \mathbb{Q}(\sqrt{D})$. This fact, together with Lemma B.0.4, show that the discriminant of an order in a quadratic field determines it uniquely. It is also straightforward that every $D \equiv 0, 1 \pmod 4$ is the discriminant of some order in some quadratic field.

From now on $\mathcal{O}$ will always be an order in K with conductor f and discriminant D.

Let us recall the definition of fractional ideal. If A is a ring and F is its field of fractions, then a *fractional ideal of* A is an A-submodule I of F such that $dI \subseteq A$ for some $d \in A$. If A is Noetherian (as is the case of an order in a number field) it is equivalent to say that I is a finitely generated A-submodule of F. We say that a fractional A-ideal $\mathfrak{a}$ is *invertible* if there exists some fractional ideal $\mathfrak{b}$ of A such that $\mathfrak{a}\mathfrak{b} = A$ (and, in this case, we write $\mathfrak{b} = \mathfrak{a}^{-1}$).

Definition B.0.6. A fractional ideal $\mathfrak{a}$ of $\mathcal{O}$ is *proper* if it satisfies the following condition:

$$\{\beta \in K : \beta\mathfrak{a} \subseteq \mathfrak{a}\} = \mathcal{O} .$$

Remark 41. The inclusion $\mathcal{O} \subseteq \{\beta \in K : \beta\mathfrak{a} \subseteq \mathfrak{a}\}$ always holds, so that we must only check the opposite inclusion.

Clearly, all principal fractional $\mathcal{O}$-ideals are proper. Also observe that, since any fractional ideal $\mathfrak{a}$ of $\mathcal{O}$ is a finitely generated $\mathcal{O}$-module, for any $\beta \in K$ the condition $\beta\mathfrak{a} \subseteq \mathfrak{a}$ implies that β is integral over $\mathcal{O}$ and therefore $\beta \in \mathcal{O}_K$. In particular, if $\mathcal{O} = \mathcal{O}_K$ we see that all fractional ideals are proper.

Lemma B.0.7. Assume that $K = \mathbb{Q}(\tau)$, where τ is a root of the polynomial $aX^2 + bX + c$ with integer relatively prime coefficients. Then $\mathbb{Z}\langle 1, \tau\rangle$ is a proper fractional ideal of the order $\mathbb{Z}\langle 1, a\tau\rangle$.

Proof. Observe that $a\tau$ is a root of $X^2 + bX + ac$, so that $a\tau$ is an algebraic integer and $\mathbb{Z}\langle 1, a\tau\rangle$ is an order in K. For $\beta \in K$, the condition $\beta\mathbb{Z}\langle 1, \tau\rangle \subseteq \mathbb{Z}\langle 1, \tau\rangle$ is equivalent to the pair of conditions

$$\begin{aligned} \beta \cdot 1 &\in \mathbb{Z}\langle 1, \tau\rangle \\ \beta \cdot \tau &\in \mathbb{Z}\langle 1, \tau\rangle \,. \end{aligned}$$

The first of these conditions simply says that $\beta = m + n\tau$ for some $m, n \in \mathbb{Z}$. For the second one, observe that

$$\beta\tau = m\tau + n\tau^2 = -\frac{cn}{a} + \left(-\frac{bn}{a} + m\right)\tau \,,$$

so that, since a, b and c are relatively prime integers, we have that $\beta \cdot \tau \in \mathbb{Z}\langle 1, \tau\rangle$ if and only if a divides n. Hence, we have seen that the condition $\beta\mathbb{Z}\langle 1, \tau\rangle \subseteq \mathbb{Z}\langle 1, \tau\rangle$ is equivalent to the condition that β be of the form $m + da\tau$ for some $m, d \in \mathbb{Z}$, i.e. $\beta \in \mathbb{Z}\langle 1, a\tau\rangle$. □

For any $\beta \in K$ and for any fractional ideal $\mathfrak{a}$ of K, we denote by β' and $\mathfrak{a}'$ their images under the non-trivial $\mathbb{Q}$-automorphism of K.

Proposition B.0.8. A fractional $\mathcal{O}$-ideal $\mathfrak{a}$ is invertible if and only if it is proper.

Proof. Assume first that $\mathfrak{a}$ is invertible. Then, for any $\beta \in K$ such that $\beta\mathfrak{a} \subseteq \mathfrak{a}$, we have

$$\beta\mathcal{O} = \beta\left(\mathfrak{a}\mathfrak{a}^{-1}\right) = (\beta\mathfrak{a})\mathfrak{a}^{-1} \subseteq \mathfrak{a}\mathfrak{a}^{-1} = \mathcal{O} \,,$$

which shows that $\beta \in \mathcal{O}$.

Now, assume that $\mathfrak{a}$ is proper. Since $\mathfrak{a}$ is a fractional ideal, we have $d\mathfrak{a} \subseteq \mathcal{O}$ for some $d \in \mathcal{O}$. It is clear that $\mathfrak{a}$ contains a $\mathbb{Q}$-basis of K. Then, since $\mathcal{O}$ is a free $\mathbb{Z}$-module of rank 2, so is $\mathfrak{a}$, so that $\mathfrak{a} = \mathbb{Z}\langle\alpha, \beta\rangle$ for some $\alpha, \beta \in K$. Defining $\tau = \beta/\alpha$, we have $\mathfrak{a} = \alpha\mathbb{Z}\langle 1, \tau\rangle$. Let $aX^2 + bX + c$ be an integer multiple of the minimum polynomial of τ with integer relatively prime coefficients. Then, by the previous lemma, we have $\mathcal{O} = \mathbb{Z}\langle 1, a\tau\rangle$. Since τ' is also a root of $aX^2 + bX + c$, we have $\mathfrak{a}' = \alpha'\mathbb{Z}\langle 1, \tau'\rangle$, which shows that $\mathfrak{a}'$ is a proper fractional ideal of $\mathbb{Z}\langle 1, a\tau'\rangle = \mathbb{Z}\langle 1, a\tau\rangle = \mathcal{O}$ (we have used that $a\tau + a\tau' = -b$). Observe that

$$\begin{aligned} a\mathfrak{a}\mathfrak{a}' &= \mathrm{Nm}_{K/\mathbb{Q}}(\alpha)\mathbb{Z}\langle a, a\tau, a\tau', a\tau\tau'\rangle = \mathrm{Nm}_{K/\mathbb{Q}}(\alpha)\mathbb{Z}\langle a, a\tau, -b, c\rangle = \\ &= \mathrm{Nm}_{K/\mathbb{Q}}\mathbb{Z}\langle 1, a\tau\rangle = \mathrm{Nm}_{K/\mathbb{Q}}(\alpha)\mathcal{O} \end{aligned}$$

(in the second equality we have used that $\tau + \tau' = -b/a$ and $\tau\tau' = c/a$, and in the third equality we have used that $\gcd(a, b, c) = 1$). This clearly shows that $\mathfrak{a}$ is invertible. □

As a consequence of the previous proposition, the set of proper ideals of $\mathcal{O}$, which we will denote by $I(\mathcal{O})$, forms a commutative group under multiplication. The set of principal ideals, which we will denote by $P(\mathcal{O})$, forms a subgroup of $I(\mathcal{O})$. We define the *ideal class group of* $\mathcal{O}$

as the quotient group $Cl(\mathcal{O}) = I(\mathcal{O})/P(\mathcal{O})$. Note that, when $\mathcal{O} = \mathcal{O}_K$, the ideal class group $Cl(\mathcal{O})$ coincides with the usual ideal class group Cl_K.

As in the proof of Proposition B.0.2, we can see that any ideal $\mathfrak{a}$ of $\mathcal{O}$ has finite index in $\mathcal{O}$. Then, we define the norm of an ideal $\mathfrak{a}$ of $\mathcal{O}$ as $N(\mathfrak{a}) = |\mathcal{O}/\mathfrak{a}|$. To simplify the notation, we will also write N for $\mathrm{Nm}_{K/\mathbb{Q}}$.

Lemma B.0.9. The norm satisfies the following properties:

1. $N(\alpha\mathcal{O}) = |N(\alpha)|$ for all non-zero $\alpha \in \mathcal{O}$.
2. $N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b})$ for any proper ideals $\mathfrak{a}$ and $\mathfrak{b}$ of $\mathcal{O}$.
3. $\mathfrak{aa}' = N(\mathfrak{a})\mathcal{O}$ for any proper ideal $\mathfrak{a}$ of $\mathcal{O}$.

Proof. Take any non-zero $\alpha \in \mathcal{O}$. Since $\mathcal{O}$ is a free $\mathbb{Z}$-module of rank 2, so is $\alpha\mathcal{O}$. Then, since $\alpha\mathcal{O}$ is a $\mathbb{Z}$-submodule of $\mathcal{O}$, there exist some $\gamma_1, \gamma_2 \in \mathcal{O}$ and some positive $c_1, c_2 \in \mathbb{Z}$ such that $\mathcal{O} = \mathbb{Z}\langle\gamma_1, \gamma_2\rangle$ and $\alpha\mathcal{O} = \mathbb{Z}\langle c_1\gamma_1, c_2\gamma_2\rangle$. Clearly $|\mathcal{O}/\alpha\mathcal{O}| = c_1c_2$. On the other hand, let $u : \mathcal{O} \to \alpha\mathcal{O}$ be the $\mathbb{Z}$-linear map defined by $u(\gamma_1) = c_1\gamma_1$ and $u(\gamma_2) = c_2\gamma_2$, and let $v : \alpha\mathcal{O} \to \alpha\mathcal{O}$ be the $\mathbb{Z}$-linear map defined by $v(c_1\gamma_1) = \alpha\gamma_1$ and $v(c_2\gamma_2) = \alpha\gamma_2$. Since clearly $\mathbb{Z}\langle\alpha\gamma_1, \alpha\gamma_2\rangle = \mathcal{O}$, the map v is invertible, so that $\det(v) = \pm 1$. Then $\det(v \circ u) = \pm c_1c_2$. But $v \circ u$ is multiplication by α, which shows that $|N(\alpha)| = c_1c_2 = N(\alpha\mathcal{O})$.

Given any non-zero $\alpha \in \mathcal{O}$ and any proper ideal $\mathfrak{a}$ of $\mathcal{O}$, it is straightforward that the sequence

$$0 \longrightarrow \alpha\mathcal{O}/\alpha\mathfrak{a} \longrightarrow \mathcal{O}/\alpha\mathfrak{a} \longrightarrow \mathcal{O}/\alpha\mathcal{O} \longrightarrow 0$$

is exact, so that we get $|\mathcal{O}/\alpha\mathfrak{a}| = |\alpha\mathcal{O}/\alpha\mathfrak{a}||\mathcal{O}/\alpha\mathcal{O}|$. Since multiplication by α clearly induces an isomorphism $\mathcal{O}/\mathfrak{a} \simeq \alpha\mathcal{O}/\alpha\mathfrak{a}$, using the first statement in the lemma we get

$$N(\alpha\mathfrak{a}) = |N(\alpha)|N(\mathfrak{a})\,.$$

Now, let $\mathfrak{a}$ be a proper ideal of $\mathcal{O}$ and let us write it as in the proof of the previous proposition as $\mathfrak{a} = \alpha\mathbb{Z}\langle 1, \tau\rangle$, where τ is a root of the polynomial with integer relatively prime coefficients $aX^2 + bX + c$. Then, we have $\mathcal{O} = \mathbb{Z}\langle 1, a\tau\rangle$, so that it is clear that $N(\mathbb{Z}\langle a, a\tau\rangle) = |a|$. From the equality $a\mathfrak{a} = \alpha\mathbb{Z}\langle a, a\tau\rangle$ we get $a^2N(\mathfrak{a}) = N(\alpha)|a|$, which combined with the result $a\mathfrak{aa}' = N(\alpha)\mathcal{O}$ obtained throughout the proof of the previous proposition, yields $\mathfrak{aa}' = N(\mathfrak{a})\mathcal{O}$.

Finally, to prove the second statement, observe that for proper ideals $\mathfrak{a}$ and $\mathfrak{b}$ of $\mathcal{O}$,

$$N(\mathfrak{ab})\mathcal{O} = \mathfrak{ab}\mathfrak{a}'\mathfrak{b}' = \mathfrak{aa}'\mathfrak{bb}' = N(\mathfrak{a})\mathcal{O} \cdot N(\mathfrak{b})\mathcal{O} = N(\mathfrak{a})N(\mathfrak{b})\mathcal{O}\,.$$

□

We now present some basic notions of quadratic forms with coefficients in $\mathbb{Z}$. A *quadratic form with coefficcients in* $\mathbb{Z}$, and, from now on, simply a *form*, is a polynomial of the form $f(X, Y) = aX^2 + bXY + cY^2$, with $a, b, c \in \mathbb{Z}$. It is *primitive* if $\gcd(a, b, c) = 1$. We say that a form $f(X, Y)$ *represents* an integer m if there exist some integers x, y such that $f(x, y) = m$, and that $f(X, Y)$ *properly represents* m if x and y can be chosen to be relatively prime. The *discrimimant* of a form $f(X, Y) = aX^2 + bXY + cY^2$ is $b^2 - 4ac$.

Proposition B.0.10. Fix a square root $\sqrt{D}$ of D. If $f(X, Y) = aX^2 + bXY + cY^2$ is a primitive form of discriminant D, then $\mathbb{Z}\langle a, (-b+\sqrt{D})/2\rangle$ is a proper ideal of $\mathcal{O}$. Moreover, this assignment defines a surjective map from the set of primitive forms of discriminant D to $Cl(\mathcal{O})$, and it holds that if a primitive form of discriminant D represents some non-zero integer m, then $|m|$ is the norm of some ideal in the corresponding class in $Cl(\mathcal{O})$.

Proof. Let τ be a root of $f(X,1) = aX^2 + bX + c$. Since $f(X,Y)$ has discriminant D, we can take $\tau = (-b + \sqrt{D})/(2a)$, so that

$$\mathbb{Z}\langle a, (-b+\sqrt{D})/2\rangle = \mathbb{Z}\langle a, a\tau\rangle = a\mathbb{Z}\langle 1, \tau\rangle\,.$$

Then, by Lemma B.0.7, we see that $\mathbb{Z}\langle a, (-b+\sqrt{D})/2\rangle$ is a proper ideal of the order $\mathbb{Z}\langle 1, a\tau\rangle$, so we need only prove that $\mathcal{O} = \mathbb{Z}\langle 1, a\tau\rangle$. But observe that

$$a\tau = \frac{-b+\sqrt{D}}{2} = \frac{-b+f\sqrt{d_K}}{2} = -\frac{b+fd_K}{2} + fw_K\,,$$

where $(b+fd_K)/2$ is an integer since $f^2 d_K = D = b^2 - 4ac$ and therefore b and fd_K have both the same parity. Then, clearly

$$\mathbb{Z}\langle 1, a\tau\rangle = \mathbb{Z}\langle 1, fw_K\rangle = \mathcal{O}\,.$$

To prove surjectivity, let $\mathfrak{a} = \alpha\mathbb{Z}\langle 1, \tau\rangle$ be a proper ideal of $\mathcal{O}$. Let $aX^2 + bX + c$ be a non-zero integer multiple of the minimal polynomial of τ with integer relatively prime coefficients. Then $\mathfrak{a}$ is proper in $\mathbb{Z}\langle 1, a\tau\rangle$, which implies that $\mathcal{O} = \mathbb{Z}\langle 1, a\tau\rangle$ and hence that $D = b^2 - 4ac$. We can assume that $\tau = (-b+\sqrt{D})/2$ by simply changing τ by $-\tau$ and b by $-b$ if $\tau = (-b-\sqrt{D})/(2a)$. Then, the primitive form $f(X,Y) = aX^2 + bXY + cY^2$ maps to $a\mathbb{Z}\langle 1, \tau\rangle$, which clearly lies in the same class in $C(\mathcal{O})$ as $\mathfrak{a}$.

Now, let $f(X,Y) = aX^2 + bXY + cY^2$ be a primitive form of discriminant D, let m be a non-zero integer and assume that $f(x,y) = m$ for some $x, y \in \mathbb{Z}$. Define $d = \gcd(x,y)$. Then $m = d^2 t$, where $t = f(x/d, y/d)$ is properly represented by $f(X,Y)$. Define $p = x/d$ and $q = y/d$. Using Bézout's lemma, there exist some $r, s \in \mathbb{Z}$ such that $ps - qr = 1$. Define $\tau = (-b+\sqrt{D})/(2a)$. Then $f(X,Y)$ maps to the class of $\mathfrak{a} = a\mathbb{Z}\langle 1, \tau\rangle$ and we have $\mathcal{O} = \mathbb{Z}\langle 1, a\tau\rangle$. Observe that

$$\begin{aligned} N(q\tau - p) &= \left(-p - \frac{qb}{2a} + \frac{q}{2a}\sqrt{D}\right)\left(-p - \frac{qb}{2a} - \frac{q}{2a}\sqrt{D}\right) \\ &= \left(p + \frac{qb}{2a}\right)^2 - \left(\frac{q}{2a}\right)^2 (b^2 - 4ac) = \frac{t}{a}\,, \end{aligned}$$

so that

$$\begin{aligned} t\frac{s\tau - r}{q\tau - p} &= t\frac{(s\tau - r)(q\tau' - p)}{N(q\tau - p)} = a\left(sq\frac{c}{a} - sp\tau - rq\left(-\frac{b}{a} - \tau\right) + rp\right) \\ &= sqc - a\tau + rqb + sp \end{aligned}$$

and, therefore,

$$\mathcal{O} = \mathbb{Z}\left\langle 1, t\frac{s\tau - r}{q\tau - p}\right\rangle\,.$$

The ideal

$$\mathfrak{b} = t\mathbb{Z}\left\langle 1, \frac{s\tau - r}{q\tau - p}\right\rangle$$

has clearly index $|t|$ in $\mathcal{O}$, so that $N(\mathfrak{b}) = |t|$ and it lies in the same class as $\mathfrak{a}$ because we have

$$t\mathbb{Z}\left\langle 1, \frac{s\tau - r}{q\tau - p}\right\rangle = \frac{t}{q\tau - p}\mathbb{Z}\langle q\tau - p, s\tau - r\rangle = \frac{t}{q\tau - p}\mathbb{Z}\langle 1, \tau\rangle\,.$$

Finally $N(d\mathfrak{b}) = d^2 N(\mathfrak{b}) = |m|$. □

Corollary B.0.11. Let M be a non-zero integer. Then, every class in $Cl(\mathcal{O})$ contains some ideal of norm relatively prime to M.

Proof. In view of the previous proposition, it suffices to prove that every primitive form represents integers relatively prime to M. So let $f(X,Y) = aX^2 + bXY + cY^2$ be a primitive form. Since $\gcd(a,b,c) = 1$, for every prime $p \mid M$ at least one of the numbers $f(1,0) = a$, $f(0,1) = c$ and $f(1,1) = a + b + c$ is relatively prime to p. Then, the result follows by a simple application of the Chinese remainder theorem. □

Now, we will study the ideals of $\mathcal{O}$ prime to the conductor, i.e. the ideals $\mathfrak{a}$ such that $\mathfrak{a} + f\mathcal{O} = \mathcal{O}$.

Lemma B.0.12. An ideal $\mathfrak{a}$ of $\mathcal{O}$ is prime to an integer m (i.e. it is prime to $m\mathcal{O}$) if and only if its norm is relatively prime to m.

Proof. The map $\mathcal{O}/\mathfrak{a} \to \mathcal{O}/\mathfrak{a}$ defined as multiplication by m is surjective (and hence an isomorphism, because $\mathcal{O}/\mathfrak{a}$ is finite) if and only if $\mathfrak{a} + m\mathcal{O} = \mathcal{O}$. But since $\mathcal{O}/\mathfrak{a}$ is a finite group, multiplication by m defines an isomorphism if and only if m is relatively prime to the order of the group, i.e. if and only if m is relatively prime to $N(\mathfrak{a})$. □

Lemma B.0.13. Every ideal of $\mathcal{O}$ prime to f is proper.

Proof. Let $\mathfrak{a}$ be an ideal prime to f. Any $\beta \in K$ such that $\beta\mathfrak{a} \subseteq \mathfrak{a}$ is an algebraic integer, because $\mathfrak{a}$ is a finitely generated $\mathbb{Z}$-module. Then, for such a β we have

$$\beta\mathcal{O} = \beta(\mathfrak{a} + f\mathcal{O}) \subseteq \mathfrak{a} + f\mathcal{O}_K\,,$$

and the result follows since $f\mathcal{O}_K \subseteq \mathcal{O}$ (because $\mathcal{O}$ has index f in $\mathcal{O}_K$). □

Because of the multiplicativity of the norm of ideals (Lemma B.0.9), the two previous lemmas imply that the set of ideals of $\mathcal{O}$ prime to f generate a subgroup of $I(\mathcal{O})$, which will be denoted by $I(\mathcal{O}, f)$. If $\mathcal{O} = \mathcal{O}_K$, then $I(\mathcal{O}, f) = I_K(f)$ The subgroup of $I(\mathcal{O}, f)$ generated by the principal ideals $\alpha\mathcal{O}$ with $N(\alpha)$ relatively prime to f will be denoted by $P(\mathcal{O}, f)$.

Proposition B.0.14. The inclusion $I(\mathcal{O}, f) \hookrightarrow I(\mathcal{O})$ induces an isomorphism

$$I(\mathcal{O}, f)/P(\mathcal{O}, f) \simeq Cl(\mathcal{O})\,.$$

Proof. The map $I(\mathcal{O}, f) \to Cl(\mathcal{O})$ is surjective because of Corollary B.0.11, so that we need only prove that $I(\mathcal{O}, f) \cap P(\mathcal{O}) = P(\mathcal{O}, f)$. The inclusion $P(\mathcal{O}, f) \subseteq I(\mathcal{O}, f) \cap P(\mathcal{O})$ is obvious, so let us focus on the opposite one. Any element of $I(\mathcal{O}, f) \cap P(\mathcal{O})$ can be written as $\mathfrak{a}\mathfrak{b}^{-1}$ with $\mathfrak{a}$ and $\mathfrak{b}$ ideals of $\mathcal{O}$ prime to f, and can also be written as $\alpha\mathcal{O}$ for some $\alpha \in K$. Lemma B.0.9 shows that $N(\mathfrak{b})\mathfrak{b}^{-1} = \mathfrak{b}'$. Then, we get

$$N(\mathfrak{b})\alpha\mathcal{O} = N(\mathfrak{b})\mathfrak{a}\mathfrak{b}^{-1} = \mathfrak{a}\mathfrak{b}'\,,$$

whereby $N(\mathfrak{b})\alpha\mathcal{O} \in P(\mathcal{O}, f)$ and therefore $N(\mathfrak{b})\alpha\mathcal{O} \cdot (N(\mathfrak{b})\mathcal{O})^{-1} \in P(\mathcal{O}, f)$. □

Given an integer m, we will use the notation $I_K(m)$ to denote the subgroup of I_K generated by the ideals prime to m (this is the same notation used previously, if we think of m as a modulus).

Proposition B.0.15. The map $\mathfrak{a} \mapsto \mathfrak{a} \cap \mathcal{O}$ induces an isomorphism $I_K(f) \xrightarrow{\simeq} I(\mathcal{O}, f)$. Its inverse is induced by $\mathfrak{a} \mapsto \mathfrak{a}\mathcal{O}_K$. Moreover, this isomorphism matches (integral) ideals of the same norm.

Proof. Let $\mathfrak{a}$ be an ideal of $\mathcal{O}_K$ prime to f. The map $\mathcal{O}/\mathfrak{a} \to \mathcal{O}_K/\mathfrak{a}$ is clearly injective, and it is also surjective because $\mathcal{O}_K = \mathfrak{a} + f\mathcal{O}_K$ and $f\mathcal{O}_K \subseteq \mathcal{O}$. Hence $N(\mathfrak{a} \cap \mathcal{O}) = N(\mathfrak{a})$ and consequently $\mathfrak{a} \cap \mathcal{O}$ is prime to f.

Now let $\mathfrak{a}$ be an ideal of $\mathcal{O}$ prime to f. Then

$$\mathfrak{a}\mathcal{O}_K + f\mathcal{O}_K = (\mathfrak{a} + f\mathcal{O})\mathcal{O}_K = \mathcal{O}_K\,,$$

which shows that $\mathfrak{a}\mathcal{O}_K$ is also prime to f.

For an ideal $\mathfrak{a}$ of $\mathcal{O}$ prime to f, we clearly have $\mathfrak{a} \subseteq \mathfrak{a}\mathcal{O}_K \cap \mathcal{O}$, and, to prove the opposite inclusion, observe that

$$\mathfrak{a}\mathcal{O}_K \cap \mathcal{O} = (\mathfrak{a}\mathcal{O}_K \cap \mathcal{O})\mathcal{O} = (\mathfrak{a}\mathcal{O}_K \cap \mathcal{O})(\mathfrak{a} + f\mathcal{O}) \subseteq \mathfrak{a} + \mathfrak{a} \cdot f\mathcal{O}_K \subseteq \mathfrak{a}\,.$$

For an ideal $\mathfrak{a}$ of $\mathcal{O}_K$ prime to f, we clearly have $(\mathfrak{a} \cap \mathcal{O})\mathcal{O}_K \subseteq \mathfrak{a}$, and for the opposite inclusion,

$$\mathfrak{a} = \mathfrak{a}\mathcal{O} = \mathfrak{a}(\mathfrak{a} \cap \mathcal{O} + f\mathcal{O}) \subseteq (\mathfrak{a} \cap \mathcal{O})\mathcal{O}_K + f\mathfrak{a} \subseteq (\mathfrak{a} \cap \mathcal{O})\mathcal{O}_K$$

(for the last inclusion we have used $f\mathfrak{a} \subseteq f\mathcal{O}_K \subseteq \mathcal{O}$).

We have seen that the maps $\mathfrak{a} \mapsto \mathfrak{a} \cap \mathcal{O}$ and $\mathfrak{a} \mapsto \mathfrak{a}\mathcal{O}_K$ provide a bijection between the monoid of ideals of $\mathcal{O}_K$ prime to f and the monoid of ideals of $\mathcal{O}$ prime to f. This bijection matches ideals of the same norm, as we have seen that for an ideal $\mathfrak{a}$ of $\mathcal{O}_K$ prime to f, its image $\mathfrak{a} \cap \mathcal{O}$ has the same norm. Moreover, this bijection is multiplicative, since the map $\mathfrak{a} \mapsto \mathfrak{a}\mathcal{O}_K$ clearly is, and therefore it induces an isomorphism $I_K(f) \simeq I(\mathcal{O}, f)$. □

Remark 42. In the previous proposition we proved that for any ideal $\mathfrak{a}$ of $\mathcal{O}_K$ prime to f we have an isomorphism $\mathcal{O}/\mathfrak{a} \cap \mathcal{O} \simeq \mathcal{O}_K/\mathfrak{a}$. Then, because of the proposition, for all ideal $\mathfrak{a}$ of $\mathcal{O}$ prime to f we have an isomorphism $\mathcal{O}/\mathfrak{a} \simeq \mathcal{O}_K/\mathfrak{a}\mathcal{O}_K$, so that $\mathfrak{a}$ is a prime ideal of $\mathcal{O}$ if and only if $\mathfrak{a}\mathcal{O}_K$ is a prime ideal of $\mathcal{O}_K$. This allows to prove that every ideal of $\mathcal{O}$ prime to f has a unique factorization as a product of prime ideals prime to f.

We define $P_{K,\mathbb{Z}}(f)$ as the subgroup of $I_K(f)$ generated by the principal ideals $\alpha\mathcal{O}_K$ with $\alpha \in \mathcal{O}_K$ and $\alpha \equiv a \pmod{f\mathcal{O}_K}$ for some $a \in \mathbb{Z}$ relatively prime to f.

Proposition B.0.16. There are natural isomorphisms

$$Cl(\mathcal{O}) \simeq I(\mathcal{O}, f)/P(\mathcal{O}, f) \simeq I_K(f)/P_{K,\mathbb{Z}}(f)\,.$$

Proof. The first isomorphism is the one in Proposition B.0.14. For the second one, we have seen in the previous proposition that the map $\mathfrak{a} \mapsto \mathfrak{a}\mathcal{O}_K$ induces an isomorphism $I(\mathcal{O}, f) \xrightarrow{\simeq} I_K(f)$, so we need only prove that $P(\mathcal{O}, f)$ maps to $P_{K,\mathbb{Z}}(f)$.

To that end, we claim that for any $\alpha \in \mathcal{O}_K$,

$$\alpha \equiv a \pmod{f\mathcal{O}_K} \text{ for some } a \in \mathbb{Z} \text{ with } \gcd(a, f) = 1 \Leftrightarrow \alpha \in \mathcal{O} \text{ and } \gcd(N(\alpha), f) = 1. \quad \text{(B.1)}$$

Assume that $\alpha \equiv a \pmod{f\mathcal{O}_K}$ for some $a \in \mathbb{Z}$ with $\gcd(a, f) = 1$. Since $f\mathcal{O}_K \subseteq \mathcal{O}$, this clearly implies $\alpha \in \mathcal{O}$. We also deduce that $\alpha' \equiv a \pmod{f\mathcal{O}_K}$, so that $N(\alpha) = \alpha\alpha' \equiv a^2 \pmod{f\mathcal{O}_K}$. Since $f\mathcal{O}_K \cap \mathbb{Z} = f\mathbb{Z}$, we get $N(\alpha) \equiv a^2 \pmod{f}$, whereby we deduce $\gcd(N(\alpha), f) = 1$. Conversely, assume that $\alpha \in \mathcal{O}$ and $\gcd(N(\alpha), f) = 1$. Since $\mathcal{O} = \mathbb{Z}\langle 1, fw_K\rangle$, we see that $\alpha \equiv a \pmod{f\mathcal{O}_K}$ for some $a \in \mathbb{Z}$. As previously $N(\alpha) \equiv a^2 \pmod{f}$, which shows that $\gcd(a, f) = 1$.

Since $P(\mathcal{O}, f)$ is generated by the principal ideals $\alpha\mathcal{O}$ with $\gcd(N(\alpha), f) = 1$ and $P_{K,\mathbb{Z}}(f)$ is generated by the principal ideals $\alpha\mathcal{O}_K$ with $\alpha \equiv a \pmod{f\mathcal{O}_K}$ for some $a \in \mathbb{Z}$ with $\gcd(a, f) = 1$, we obtain the desired result. □

Bibliography

[Cox13] Cox, D. A. *Primes of the Form $x^2 + ny^2$*. New York: John Wiley & Sons, Inc., 2013.

[Mil17a] Milne, J. S. *Algebraic Number Theory (v3.07)*. Available at `www.jmilne.org/math/`, 2017.

[Mil13] Milne, J. S. *Class Field Theory (v4.02)*. Available at `www.jmilne.org/math/`, 2013.

[Mil17b] Milne, J. S. *Fields and Galois Theory (v4.53)*. Available at `www.jmilne.org/math/`, 2017.

[Neu99] Neukirch, J. *Algebraic Number Theory*. Translated by Norbert Schappacher. Berlin and Heidelberg: Springer-Verlag, 1999.

[Neu86] Neukirch, J. *Class Field Theory*. Translated by Lemmermeyer, F., and Snyder, W. Berlin and Heidelberg: Springer-Verlag, 1986.

[Sam70] Samuel, P. *Algebraic Theory of Numbers*. Translated by Silberger, Allan J. Paris: Hermann, 1970.

[Ser67] Serre, J-P. "Local Class Field Theory." In *Algebraic Number Theory*, edited by Cassels, J. W. S., and Fröhlich, A. Washington, D.C.: Thomson Book Company Inc., 1967.

[Ser79] Serre, J-P. *Local fields*. Translated by Greenberg, M. J. New York: Springer-Verlag, 1979.

[Tat67] Tate, J. T. "Global Class Field Theory." In *Algebraic Number Theory*, edited by Cassels, J. W. S., and Fröhlich, A. Washington, D.C.: Thomson Book Company Inc., 1967.